21世纪高等院校计算机网络工程专业规划教材

网络安全与管理

石磊 赵慧然 编著

可下载教学资料
http://www.tup.tsinghua.edu.cn

清华大学出版社



21世纪高等院校网络工程专业规划教材

网络安全与管理

石　磊　赵慧然　编著

清华大学出版社
北　京

内 容 简 介

本书是根据作者多次讲授"网络安全"课程的教学经验以及进行实验指导的体会编写而成的。本书从实践出发，以基本理论的应用和网络安全工具的使用为中心，以理论讲述为基础，避免了一些传统网络安全教材理论过多、理论过难、操作性不强、理论和实际联系不紧的问题，重点介绍网络安全领域的最新问题和工具的运用。

全书分理论部分9章和实验部分6章。理论部分是对网络安全体系结构和技术的详细讲解，通过这一部分使学生在理论上有一个清楚的认识，每章后面都有各类习题供学生总结和复习所学的知识；实验部分选择了目前常用的几种网络安全工具，通过对工具的使用与操作，达到理解运用的目的。附录中还提供了一个完整的应用系统网络安全解决方案，将网络安全理论知识与现实的工程项目综合起来，以便学生"看懂、学会、用上"。

本书可作为网络工程、计算机、信息安全等专业本科生的教科书与实验教材，也可供从事相关专业的教学、科研和工程人员参考。

本书配套的电子课件可从清华大学出版社网站(http://www.tup.com.cn)下载。

图书在版编目(CIP)数据

网络安全与管理/石磊，赵慧然编著. —北京：清华大学出版社，2009.9
(21世纪高等院校计算机网络工程专业规划教材)
ISBN 978-7-302-20561-6

Ⅰ. 网…　Ⅱ. ①石…　②赵…　Ⅲ. 计算机网络—安全技术　Ⅳ. TP393.08

中国版本图书馆CIP数据核字(2009)第151076号

责任编辑：索　梅　徐跃进
责任校对：白　蕾
责任印制：

出版发行：清华大学出版社　　**地　址：**北京清华大学学研大厦A座
http://www.tup.com.cn　　**邮　编：**100084
社 总 机：010-62770175　　**邮　购：**010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：
装 订 者：
经　销：全国新华书店
开　本：185×260　　**印　张：**18.75　　**字　数：**448千字
版　次：2009年9月第1版　　**印　次：**2009年9月第1次印刷
印　数：1～　000
定　价：　.00元

本书如存在文字不清、漏印、缺页、倒页、脱页等印装质量问题，请与清华大学出版社出版部联系调换。联系电话：010-62770177转3103　　产品编号：

前　言

21 世纪是互联网时代，网络安全的内涵发生了根本性的变化。网络安全在信息领域中的地位从一般性的防卫手段变成了非常重要的安全防御措施；网络安全技术从之前只有少部分人研究的专门领域变成了生活中无处不在的普遍应用。当人类步入 21 世纪这一信息社会的时候，网络安全问题成为互联网的焦点，我们每个人都时刻关注着与自身密不可分的网络系统的安全，从应用和管理的角度建立起一套完整的网络安全体系无论对于单位还是个人都显得尤为重要，提高网络安全意识、掌握网络安全管理工具的使用逐步提到日程上来。

"网络安全与管理"是计算机专业、网络工程专业的主要专业课，学生应从四个方面掌握网络安全的基本概念、应用技术、管理工具的使用以及解决方案的设计。

1. 网络安全的基本概念

网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或恶意的原因而遭受到破坏、更改、泄露，系统连续、可靠、正常地运行，网络服务不中断。网络安全从其本质上来讲就是网络上的信息安全；从广义上说，凡是涉及网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络安全的研究领域。本书从网络安全的各个方面进行了基本的介绍，这些介绍主要包括各种技术的概念、分类、原理、特点等知识，而对于复杂而枯燥的算法和理论研究没有作详细介绍，通过对这些知识的学习来理解网络安全体系中各部分之间的联系。

2. 网络安全应用技术

网络安全应用技术是指致力于解决诸如如何有效进行访问控制，以及如何保证数据传输的安全性的技术手段，主要包括网络监控技术、密码技术、病毒防御技术、防火墙技术、入侵检测技术、VPN 技术，及其他安全服务和安全机制策略。单一的网络安全技术和网络安全产品无法解决网络安全的全部问题，应根据应用需求和安全策略，综合运用各种网络安全技术以达到全面保护网络的要求。本书对于这些技术分章节地进行了详细介绍。

3. 网络安全管理工具

如果想对网络安全进行综合处理，就要使用多种网络安全管理工具，同时将管理工具和系统工具配合使用，才会起到事半功倍的作用。在本书的实验部分对常用的网络安全管理工具进行了相应的练习，通过学习使用这些常用的工具来理解网络安全方案的具体解决方法。

4. 网络安全解决方案设计

网络安全建设是一个系统工程，网络安全解决方案的设计直接影响到工程的质量。一个完善的解决方案应该包含哪些部分、应该提供哪些服务、如何评估方案的质量，都是学生

需要学习并理解的。在附录 A 中给出了一个网络安全解决方案，通过这个方案使学生理解如何针对一个真实的网络设计安全方案。

本书是一本以网络安全管理应用为目的，网络安全工具使用为重点，理论讲述为基础的系统性、应用性较强的网络安全教材。本教材摒弃了传统网络安全教材中理论过多、过难、实用性不强、理论和实践不配套、管理工具不通用等问题，以培养学生掌握基本网络安全理论知识和网络应用管理相结合为目的。教材从应用的角度系统讲述了网络安全所涉及的理论及技术。以网络安全管理工具的使用能力为培养目的，通过实验演练，使学生能够综合运用书中所讲授的技术进行网络信息安全方面的实践。

本书分为理论部分(9 章)和实验部分(6 章)，理论部分是对网络安全基本理论和技术的详细讲解，通过这一部分使学生在理论上有一个清楚的认识；实验部分选择了目前常用的几种网络安全工具，通过对工具的使用与操作，把理论和实践联系起来，达到理解运用的目的。

本书可作为网络工程、计算机、信息安全等专业本科生的教科书，也可供从事相关专业的教学、科研和工程人员参考。

本书至少需要 48 学时来进行学习，其中理论授课 24 学时，实验 24 学时，在每章的后面都有习题以供学生总结和复习所学的知识，并在附录中给出了习题答案。

本书由石磊主编，其中第 3 章、第 4 章和实验 3 由赵慧然编写。由于作者水平有限，不当之处敬请读者提出宝贵意见。

在本书编写过程中，计算机工程学院李彤院长、张坤副院长、网络工程系主任肖建良给予了作者深切的关怀与鼓励，对于本书的编写提供了帮助与指导，在此表示衷心的感谢。

编　者

2009 年 7 月

目　　录

第 1 章　网络安全概述

1.1　互联网介绍

因特网(Internet,又称网际网、国际互联网),即广域网、局域网及单机按照一定的通信协议组成的国际计算机网络。互联网是指将两台计算机或者是两台以上的计算机终端、客户端、服务端通过计算机信息技术的手段互相联系起来计算机网络。通过互联网人们可以与远在千里之外的朋友相互发送邮件,共同完成一项工作,共同娱乐。其实,人们通常所说的互联网,都是指因特网,或者说是包含因特网的,本书所提的互联网,也正是包含因特网的计算机网络。

1995 年 10 月 24 日,联合网络委员会通过了一项关于“互联网定义”的决议,联合网络委员会认为,下述语言反映了对“互联网”这个词的定义。

“互联网”指的是全球性的信息系统:

(1) 通过全球性的唯一的地址逻辑地链接在一起,这个地址是建立在互联网协议(IP)或今后其他协议基础之上的。

(2) 可以通过传输控制协议和互联网协议(TCP/IP),或者今后其他接替的协议或与互联网协议(IP)兼容的协议来进行通信。

(3) 可以让公共用户或者私人用户使用高水平的服务,这种服务是建立在上述通信及相关的基础设施之上的。

这当然是从技术的角度来定义互联网。这个定义至少揭示了三个方面的内容:首先,互联网是全球性的;其次,互联网上的每一台主机都需要有“地址”;最后,这些主机必须按照共同的规则(协议)连接在一起。

1.1.1　互联网的影响

互联网是全球性的。这就意味着人们目前使用的这个网络(不管是谁发明了它)是属于全人类的。这种“全球性”并不是一个空洞的政治口号,而是有其技术保证的。互联网的结构是按照“包交换”的方式连接的分布式网络。因此,在技术的层面上,互联网绝对不存在中央控制的问题。也就是说,不可能存在某一个国家或者某一个利益集团通过某种技术手段来控制互联网的问题。反过来,也无法把互联网封闭在一个国家之内(除非建立的不是互联网)。

然而,这样一个全球性的网络,必须要有某种方式来确定连入其中的每一台主机在互联网上绝对不能出现类似两个人同名的现象。这样,就要有一个固定的机构来为每一台主机确定名字,由此确定这台主机在互联网上的“地址”。但这仅仅是“命名权”,这种

确定地址的权力并不意味着控制的权力。负责命名的机构除了命名之外,并不能做更多的事情。

同样,这个全球性的网络也需要有一个机构来制定所有主机都必须遵守的交往规则(协议),否则就不可能建立起全球所有不同的计算机、不同的操作系统都能够通用的互联网。下一代 TCP/IP 协议将对网络上的信息等级进行分类,以加快传输速度(比如,优先传送浏览信息,而不是电子邮件信息)。同样,这种制定共同遵守的“协议”的权力,也不意味着控制的权力。

毫无疑问,互联网的所有这些技术特征都说明对于互联网的管理完完全全与“服务”有关,而与“控制”无关。

事实上,目前的互联网还远远不是人们经常说到的“信息高速公路”。这不仅因为目前互联网的传输速度不够,更重要的是互联网还没有定型,还一直在发展、变化。因此,任何对互联网的技术定义也只能是当下的、现时的。

与此同时,在越来越多的人加入到互联网中、越来越多地使用互联网的过程中,也会不断地从社会、文化的角度对互联网的意义、价值和本质提出新的理解。

1.1.2 互联网的意义

互联网也是一个面向公众的社会性组织。世界各地数以万计的人们可以利用互联网进行信息交流和资源共享。而又有成千上万的人自愿地花费自己的时间和精力,蚂蚁般地辛勤工作,构造出全人类所共同拥有的互联网,并允许他人去共享自己的劳动果实。互联网反映了人类所共赏的无私精神,互联网也使人们学会如何更好地和平共处。

互联网是人类社会有史以来第一个世界性的图书馆和第一个全球性论坛。任何人,无论来自世界的任何地方,在任何时候,他(她)都可以参加,互联网永远不会关闭。而且,无论是谁,永远是受欢迎的,不会由于不同的肤色、不同的穿戴、不同的宗教信仰而被排挤在外。在当今的世界里,唯一没有国界、没有歧视、没有政治的生活圈属于互联网。通过网络信息的传播,全世界任何人,不分国籍、种族、性别、年龄、贫富,互相传送经验与知识,发表意见和见解。

互联网是人类历史发展中的一个伟大的里程碑,它正在对人类社会的文明悄悄地起着越来越大的作用。也许会像瓦特发明的蒸汽机导致了一场工业革命一样,互联网将会极大地促进人类社会的进步和发展。

1.1.3 互联网网民规模

截至 2008 年 6 月底,中国网民数量达到 2.53 亿,网民规模跃居世界第一位,如图 1.1 所示,但是互联网的普及率只有 19.1%,仍然低于全球平均水平(21.1%)。中国网站数量为 191.9 万个,年增长率为 46.3%。其中 CN 下的网站数为 137 万,占总网站数的 71.4%。网上银行使用率为 23.4%,用户增长率较快,半年用户增长率达到 47.1%。但使用率远低于美国网民 53%的使用率,也低于韩国网民 39.1%的使用率。网上炒股/基金使用率为 16.9%,网上炒股/基金的使用率与中国的股市同步波动,使用率在下降,总体用户量略涨了 466 万。目前中国网民的使用率仍高于韩国网民的 5.4%,也高于美国网民的 11%

目前中国网民中接入宽带比例为 84.7%,宽带网民数已达到 2.14 亿人。中国的手机

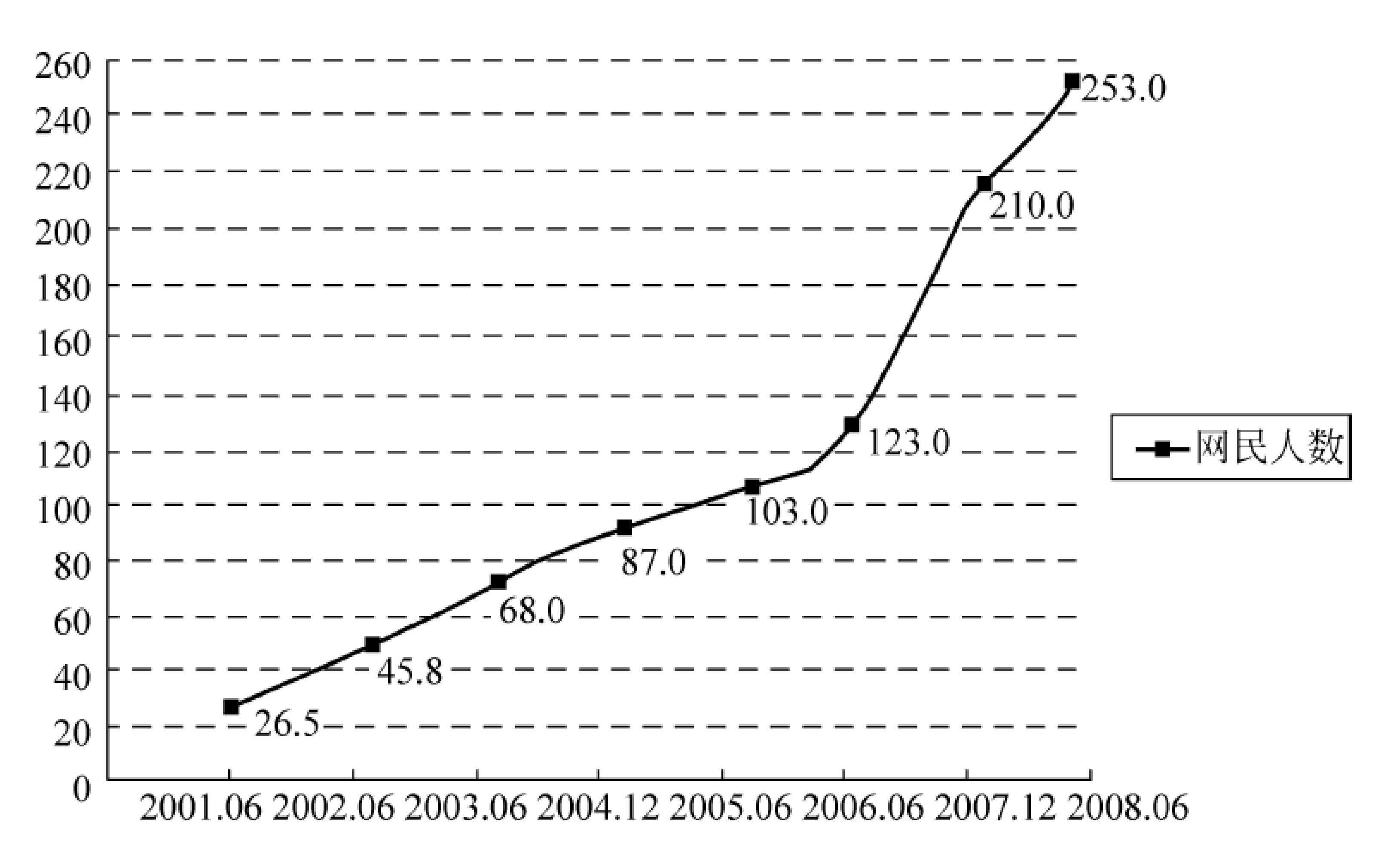


图 1.1　中国互联网网民人数(百万)

上网网民数已达到7305万人。在2.53亿网民中,半年内有过用手机接入互联网行为的网民比例达到28.9%。手机上网以其特有的便捷性,在中国发展迅速。手机上网的发展,使得网民的上网选择更加丰富,手机上网情况的变化也从一个侧面反映了网民上网条件的变化。

1.2　网络安全介绍

1.2.1　网络安全吗

这是大多数人本来就有的疑问,现在它被媒体效应放大了,而且是否定的信息大过正面。现在这个问题变成:网络那么不安全吗?

根据Nielsen//Net-Ratings公布的最新全球网际网络指数显示,亚太区的网络活动带动全球网际网络的成长。以区域计算,亚太地区的网际网络使用者之浏览页数为全球之冠。既然人们一天用在网络上的时间这么久,而且还时常必须利用它来传递个人或公司的重要信息(例如把写好的新产品上市计划书传给项目小组成员),处理与个人金钱有关的交易(例如在网络书店购书或进入网络银行进行转账),那么网络的安全问题更是每一个人所必须要重视的议题。

网络安全涉及上至国家安全下至普通百姓的计算机数据的保护,因此网络安全防范将会是每一个网络系统设计人员和管理人员的重要任务或职责。

1.2.2　网络为什么不安全

要了解网络安全,必须要先了解网络为什么不安全。基本上,不同的人对网络安全的定义不同,一般上网的使用者关心的是连上任何一台服务器时,客户端的计算机会不会被入侵或是资料被窃取的问题;而网站管理员则是集中精力在处理服务器端的网络安全问题,如何避免或延缓不良骇客的阻断攻击行为或是如何保护网站使用者资料不被窃取;进行信息流通的企业以及经营电子商店的企业和上网消费的使用者所关心的,则是如何有效运用安

全的交易平台与加密解密技术，来避免文件资料被窃取以及网络诈欺等行为的发生。

概括来说，造成网络不安全的主要原因可以分为三大类。

1. 软件本身设计不良或系统设计上的缺陷

软件本身设计不良，也就是俗称的软件有漏洞，例如使用 Internet Explorer 5.0，因为其本身设计上的疏失，使得别人很容易就可以取得一些关于使用者的重要信息。这也就是为什么常会在 Microsoft Windows Update 网站上看到某某软件的修正程序（也就是俗称的 Patch 档），或是像 Windows NT Server 常常会推出所谓的 Service Pack 的原因。利用这些漏洞，要在网站内窃取资料或是植入后门程序等，都不是很困难的事。

系统设计上的缺陷。应用程序或系统毕竟是人写出来的，所谓智者千虑，必有一失，软件设计师想的再严密，系统管理再严谨，实际应用在充满陷阱和恶意入侵的互联网上时，仍难免会有让骇客有机可乘的空隙。因此，在架设时要特别针对这些地方做补强，并配合其他防护措施，以确保网络的安全性。

Active X 带来的缺陷。Active X 控件是一种内嵌在 Web 网页的组件，当使用者浏览网页时便会被激活。在许多情况中，可将 Web 浏览器的浏览器安全设定设成“高”，来停止执行这些 Active X 控件。不过，骇客或病毒制造者以及其他恶意人士可能会使用 Active X 恶意程序代码当作武器来攻击计算机。

2. 使用者的习惯及方法不正确

谨慎设定管理员密码。很多网管人员在设定 UNIX 中的 root 与 Windows Server 中的 administrator 的密码时，通常采取不设密码或用很简单、很好记的密码，像是 abc、123 或是公司名称等，这使得保护系统的第一层使用者认证，有跟没有一样；而系统管理者的读写权限又较一般使用者大，一旦被入侵后果不堪设想。很多人习惯将账号或密码写在便利贴上，贴在计算机屏幕上，或轻易地把账号与密码告知他人，这就跟把家里钥匙挂在家门上一样！别忘了，隐患可能就在自己身边！计算机入侵者很有可能便是身边的熟人。

勿轻易开启来历不明的档案。有的用户收到来历不明的人寄的信件附件，也不管是什么就打开。有些附件是计算机病毒的隐身，一旦执行，重要档案便被杀个精光。有时则是档案本身藏有特洛伊木马程序，当使用者正在观看很有趣的动画时，入侵者早已将一只木马程序轻轻松松地放进入侵的系统中，透过这个程序便可以从远程掌控入侵的计算机，只要联机在网络上，骇客便随时可以把联网系统中重要的信息窃取到他的硬盘里。

3. 网络防护不够严谨

除了互联网与计算机系统本身的安全威胁外，经营者对互联网认识的不足往往也会让系统出现安全漏洞而不知觉。比如在公司的网站和内部网络间没有架设防火墙，或是企业经营者由于不了解网络技术，听信网络供货商的建议，认为只要装设防火墙便可安全无忧，那么就有可能忽略其他安全上的问题。

事实上，防火墙对于单纯的网络安全应用或许足够，但并非绝对安全，尤其是当网站服务越来越多时，必须与内部营运系统连接，否则将导致门户大开，安全漏洞也将接踵而至。另外，在 Windows 操作平台上作资源共享的密码认证与存取权限过于宽松，任何人都可以通过“网络邻居”找到设置共享的 PC，进而任意读写别人的共享磁盘。

上面三大类情况，每一种都有可能是系统被入侵或资料被盗取的原因。预防胜于治疗，读者应该立即排查是否犯了上面任何一项大忌，对症下药，彻底防堵所有可能的安全

死角。

1.2.3　网络安全防范

在了解了造成网络不安全的几个原因后，便可针对这些原因来做防范，使风险与威胁降到最低。一个完整的网络安全架构必须能针对企业可能会遇到的威胁做好万全的准备。IT 人员如能了解这些威胁，即可对该在何处、以何种方法配置，以使网络危害降低作出更周详的决定。

完整的网络安全架构应依不同的网络功能需求形成决策来执行。在网络设计过程中，可能需要选择具有整合功能或是特殊功能的网络设备。整合功能的设备通常较易被采用，因为可于现有的架构上执行，或是因为能与其他设备配合运作，从而提供更好的解决方案。特殊设备通常是对功能的先进性要求比较高，或是需要达到特定的效能表现。决策时必须依据所提供的功能性或整合性，选择较适当的设备。

以下介绍几个构建网络安全架构体系的要项。

1. 明确网络资源

网络安全方面常见的一个问题就是网络管理员不能得到一个关于网络的全面架构图，特别是随着网络的不断增长和变化，掌握网络完全情况就更加困难，因而给网络管理员提供一个清晰的网络监控图是十分重要的。通过这个网络结构图，可以清楚地辨识每个使用者在网络上的身份、地位、权限、位置和所处的部门，并可以清楚看出他与整个网络的对应关系。

2. 确定网络存取点

网络管理员应当了解潜在的非法入侵者会在何时、何地、以何身份进入系统。骇客和非法入侵者通常是通过网络连接、拨号存取以及配置不当的主机来入侵系统。基于网络域的安全解决方案，无论用户在网络的哪个地方都可辨别他的身份。

3. 限定存取权限

制定用户存取的范围(权限)，约束用户的存取权限，在网络中必须构筑多道屏障(包括来自内部的越权存取者)，使得非法入侵者不能自动进入整个系统，特别要注意对于网络中关键数据库或敏感地区的防范。

4. 确认安全防范

每个安全系统都有一定的设想和安全防范措施，在网络管理中必须认真地检查和确认安全，否则隐藏的问题就会成系统潜在的安全漏洞。必要时设立网络监控软件 24 小时全天候动态监测，以确保网络的安全。

5. 内部的安全问题

根据互联网计算机安全联盟的报告，有 80%的非法入侵事件来自于防火墙内部，这主要是因为目前提供的一些内部保护措施比较单一。

6. 公钥验证

目录服务除了作为网络资源的存置所外，此目录服务一方面必须能作为钥匙的存盘库，另一方面还必须提供在此目录中的对象之间互相验证的功能；而在公钥验证系统中很重要的公钥可放在目录内供人拿来作为加密及验证收发双方身份的真伪。

7. 单一登录

网络管理员可以从一个集中点实现对整个网络的存取和安全控制,这样,他们就可以管理更多的资源,从而达到提高生产效率、降低管理成本的目的。透过网络域服务器进行安全管理,不仅具有良好的伸缩性,而且允许管理员通过某些可控的安全方式,将某些存取管理的职责予以下放。单一登录也就意味着用户只需记住一个密码,从而,能够很快地获得其所需要的资源,并提高生产效率。基于网络域服务器的验证比传统的 TCP/IP 安全机制安全得多。TCP/IP 的安全性较弱,主要是因为它是基于 IP 地址或网址的,而不是基于用户本身的。

但是,尽管各类防毒软件、防火墙与内容过滤技术可协助我们监视外来威胁,却无法防止人为造成的安全漏洞而危及网络安全,所以,除了设备的选择外,还需注意人为安全漏洞的防范。以下介绍几个防止人为安全漏洞的步骤:

(1) 设立互联网使用规范。明确的互联网规范,可提高 IT 人员设定与监视网络安全的效率。

(2) 扫描邮件是否含有不适当的内容,并记录违反管制规定的行为。

(3) 教育训练。教导用户如何下载最新的防毒更新资料、如何辨认计算机是否可能中毒、教导在开启档案之前先扫描档案是否有病毒。

(4) 修补软件漏洞,降低病毒透过网页或电子邮件渗入的机会。

(5) 经常更换密码,教育用户防范社交欺骗手段,要求无论如何都不可交出密码。

预防更胜于治疗。造成网络不安全的原因非常多,人们无法得知全部,但却可以透过许多方式(例如安装防毒软件、防火墙及个人习惯的改变),来使风险与威胁降到最低。而其中最难防范的莫过于人为的疏忽,而导致人为疏忽最重要的原因即为专业知识的不足。所以,更应该随时对用户进行教育训练,以使网络安全的风险及威胁降到最低。

1.3 十大威胁企业安全的网络危险行为

据国外媒体报道,对于一家企业而言,雇员是必不可少的。但同时,雇员也是企业计算基础设施安全的最大威胁。因为大多数雇员对其在线行为的危险性不以为然。

无论对雇员进行多少次的安全知识培训,无论雇员上了多少堂课,大多数公司网管仍然对企业内网的安全感到无助和绝望。因为终端用户总是禁不住各种病毒附件的“诱惑”,为了获取浏览速度,雇员不惜关闭防火墙或者将登录密码保存在计算机中。

为了确保企业网络安全,这里列出了“10 种最危险的网络行为”,希望能够引以为戒。十大网络危险行为如下:

(1) 浏览不明邮件附件;

(2) 安装未授权应用;

(3) 关闭或禁用安全工具;

(4) 浏览不明 HTML 或文本消息;

(5) 浏览赌博、色情或其他非法站点;

(6) 公开自己的登录密码、令牌或智能卡信息;

(7) 重要的文档裸奔,没有加密;

(8) 随意访问未知、不可信站点;

(9) 随意填写 Web 脚本、表格或注册页面;

(10) 频繁访问聊天室或社交站点。

1.4 常用网络密码安全保护技巧

当前,大部分用户密码被盗,多是因为缺少网络安全保护意识以及自我保护意识,以致被黑客盗取引起经济损失。下面将介绍针对十类破解方法的对策,举出十类密码安全和保护技巧,希望可以提高网络安全意识。

1. 使用复杂的密码

密码穷举对于简单的长度较少的密码非常有效,但是如果网络用户把密码设的较长一些而且没有明显规律特征(如用一些特殊字符和数字字母组合),那么穷举破解工具的破解过程就变得非常困难,破解者往往会对长时间的穷举失去耐性。通常认为,密码长度应该至少大于 6 位,最好大于 8 位,密码中最好包含字母数字和符号,不要使用纯数字的密码,不要使用常用英文单词的组合,不要使用自己的姓名作为密码,不要使用生日作为密码。

2. 使用软键盘

对付击键记录,目前有一种比较普遍的方法就是通过软键盘输入。软键盘也叫虚拟键盘,用户在输入密码时,先打开软键盘,然后用鼠标选择相应的字母输入,这样就可以避免木马记录击键;另外,为了更进一步保护密码,用户还可以打乱输入密码的顺序,这样就进一步增加了黑客破解密码的难度。

3. 使用动态密码(一次性密码)

动态密码(dynamic password)指用户的密码按照时间或使用次数不断动态变化,每个密码只使用一次。动态密码对于截屏破解非常有效,因为即使截屏破解了密码,也仅仅破解了一个密码,下一次登录不会再使用这个密码。但鉴于成本问题,目前大多数动态密码卡都是刮纸片的那种原始的密码卡,而不是真正意义上的一次性动态密码,其安全性还是难以保证。真正的动态密码锁采用一种称为动态令牌的专用硬件,内置电源、密码生成芯片和显示屏。其中数字键用于输入用户 PIN 码,显示屏用于显示一次性密码。每次输入正确的 PIN 码,都可以得到一个当前可用的一次性动态密码。由于每次使用的密码必须由动态令牌来产生,而用户每次使用的密码都不相同,因此黑客很难计算出下一次出现的动态密码。真正的动态密码卡成本通常为 100~200 元,较高的成本限制了其大规模的使用。

4. 网络钓鱼的防范

防范钓鱼网站的方法,首先要提高警惕,不登录不熟悉的网站,不要打开陌生人的电子邮件,安装杀毒软件并及时升级病毒知识库和操作系统补丁。使用安全的邮件系统,发送重要邮件要加密,将钓鱼邮件归为垃圾邮件。IE 7 和 FireFox 有网页防钓鱼的功能,访问钓鱼网站会有提示信息。

5. 使用 SSL 防范 Sniffer

传统的网络服务程序 HTTP、FTP、SMTP、POP3 和 Telnet 等在本质上都是不安全的,因为它们在网络上用明文传送口令和数据,Sniffer(网络嗅探器)非常容易截获这些口令和

数据。对于 Sniffer，可以采用会话加密的方案，把所有传输的数据进行加密，这样 Sniffer 即使嗅探到了数据，这些加密的数据也是难以解密还原的。目前广泛应用的是 SSL（Secure Socket Layer），可以方便、安全地实现加密数据包传输。当用户输入口令时应该使用支持 SSL 协议的方式进行登录，例如 HTTPS、SFTP、SSH，而不是使用 HTTP、FTP、POP、SMTP、TELNET 等协议，以防止 Sniffer 的监听。SSL 的安全验证可以在不安全的网络中进行安全的通信。

6. 尽量不要将密码保存在本地

将密码保存在本地是个不好的习惯，很多应用软件（例如某些 FTP 等）保存的密码并没有设计得非常安全，如果本地没有一个很好的加密策略，那将给黑客破解密码大开方便之门。

7. 使用 USB Key

USB Key 是一种 USB 接口的硬件设备，它内置单片机或智能卡芯片，有一定的存储空间，可以存储用户的私钥以及数字证书。利用 USB Key 内置的公钥算法可实现对用户身份的认证。由于用户私钥保存在密码锁中，理论上使用任何方式都无法读取，因此保证了用户认证的安全性。

8. 个人密码管理

要保持严格的密码管理观念，实施定期更换密码，可每月或每季更换一次。永远不要将密码写在纸上，不要使用容易被别人猜到的密码。对一些比较难记的密码要做存储并加密，加密后的文件即使被盗，或者无意中在网络中散布，也不会导致自己的重要信息泄露出去。

9. 密码分级

对于不同的网络系统使用不同的密码，对于重要的系统使用更为安全的密码。绝对不要所有系统使用同一个密码。对于那些偶尔登录的论坛，可以设置简单的密码；对于重要的信息、电子邮件、网上银行之类，必需设置为复杂的密码。永远也不要把论坛、电子邮箱和银行账户设置成同一个密码。

10. 生物特征识别

生物特征识别技术指通过计算机，利用人体所固有的生理特征或行为特征来进行个人身份鉴定。常用的生物特征包括指纹、掌纹、虹膜、声音、笔迹、脸像等。生物特征识别是一种简单可靠的生物密码技术，生物识别技术认定的是人本身，由于每个人的生物特征具有与其他人不同的唯一性，以及在一定时期内不变的稳定性，不易被伪造和假冒，因此，可以最大限度地保证个人资料的安全。目前人体特征识别技术市场上占有率最高的是指纹机和手形机，这两种识别方式也是目前技术发展中最成熟的。

1.5　威胁网络安全的因素

1.5.1　黑客

黑客（Hacker）的定义是：“喜欢探索软件程序奥秘并从中增长其个人才干的人。他们不像绝大多数计算机使用者，只规规矩矩地了解别人指定了解的范围狭小的部分知识”。

“黑客”大都是程序员，他们对于操作系统和编程语言有着深刻的认识，乐于探索操作系统的奥秘且善于通过探索了解系统中的漏洞及其原因所在，他们恪守这样一条准则：Never damage any system（永不破坏任何系统）。他们近乎疯狂地钻研更深入的计算机系统知识并乐于与他人共享成果。他们一度是计算机发展史上的英雄，为推动计算机的发展起了重要的作用。在网络刚兴起的时候，从事黑客活动，就意味着对计算机的潜力进行智力上最大程度的发掘。国际上的著名黑客均强烈支持信息共享论，认为信息、技术和知识都应当被所有人共享，而不能为少数人所垄断。大多数黑客都具有反社会或反传统的色彩，同时，另外一个特征是十分重视团队的合作精神。

显然，“黑客”一词原来并没有丝毫的贬义成分。直到后来，少数怀着不良企图，利用非法手段获得系统访问权去闯入远程机器系统，破坏重要数据，或为了自己的私利而制造麻烦、具有恶意行为特征的人（他们其实是骇客——Crack）慢慢玷污了“黑客”的名声，“黑客”才逐渐演变成入侵者、破坏者的代名词。

“他们瞄准一台计算机，对它进行控制，然后毁坏它。”——这是1995年美国拍摄的第一部有关黑客的电影《战争游戏》中对“黑客”概念的描述。

虽然现在对黑客的准确定义仍有不同的意见，但是，从信息安全这个角度来说，“黑客”的普遍含义是特指计算机系统的非法侵入者。多数黑客都痴迷计算机，认为自己在计算机方面的天赋过人，只要自己愿意，就可毫无顾忌地非法闯入某些敏感的信息禁区或者重要网站，以窃取重要的信息资源、篡改网址信息或者删除该网址的全部内容等恶作剧行为作为一种智力的挑战而自我陶醉。

目前黑客已成为一个特殊的社会群体，在欧美有不少完全合法的黑客组织。黑客们经常召开黑客技术交流会，1997年11月，在纽约就召开了世界黑客大会，与会者达四五千人。另一方面，黑客组织在因特网上利用自己的网站介绍黑客攻击手段、免费提供各种黑客工具软件、出版网上黑客杂志。这使得普通人也很容易下载并学会使用一些简单的黑客手段或工具对网络进行某种程度的攻击，进一步恶化了网络安全环境。

1.5.2 黑客会做什么

很多人会问：“黑客平时都做什么？是不是非常刺激？”也有人对黑客的理解是“天天做无聊且重复的事情”。实际上这些又是一个错误的认识，黑客平时需要用大量的时间学习，由于学习完全出于个人爱好，所以无所谓“无聊”；重复是不可避免的，因为“熟能生巧”，只有经过不断的练习、实践，才可能自己体会出一些只可意会，不可言传的心得。

在学习之余，黑客应该将自己所掌握的知识应用到实际当中。无论是哪种黑客做出来的事情，根本目的无非是在实际中掌握自己所学习的内容。黑客的行为主要有以下几种。

1. 学习技术

互联网上的新技术一旦出现，黑客就必须立刻学习，并用最短的时间掌握这项技术。这里所说的掌握并不是一般的了解，而是阅读有关的“协议”、深入了解此技术，否则一旦停止学习，那么依靠他以前掌握的内容，并不能维持他的“黑客身份”超过一年。

初级黑客要学习知识是比较困难的，因为他们没有基础，所以学习起来要接触非常多的基本内容，然而今天的互联网给读者带来了很多的信息，这就需要初级学习者进行选择：太

深的内容可能会给学习带来困难；太“花哨”的内容又对学习黑客没有用处。

2. 伪装自己

黑客的一举一动都会被服务器记录下来，所以黑客必须伪装自己使得对方无法辨别其真实身份，这需要有熟练的技巧，用来伪装自己的 IP 地址、使用跳板逃避跟踪、清理记录扰乱对方线索、巧妙躲开防火墙等。

伪装是需要非常过硬的基本功才能实现的，这对于初学者来说是很困难的。也就是说，初学者不可能用短时间学会伪装，所以不鼓励初学者利用自己所学习的知识对网络进行攻击，否则一旦自己的行迹败露，最终受害的是自己。

3. 发现漏洞

漏洞对黑客来说是最重要的信息，黑客要经常学习别人发现的漏洞，努力寻找未知的漏洞，并从海量的漏洞中寻找有价值的、可被利用的漏洞进行试验。当然他们最终的目的是通过漏洞进行破坏或者修补上这个漏洞。

黑客对寻找漏洞的执著是常人难以想象的，他们的口号是“打破权威”。在一次又一次的黑客实践中，黑客用自己的实际行动向世人印证了这一点——世界上没有“不存在漏洞”的程序。在黑客眼中，所谓的“天衣无缝”不过是“没有找到”而已。

4. 利用漏洞

对于正派黑客来说，漏洞要修补；对于邪派黑客来说，漏洞要用来搞破坏。而他们的基本前提是“利用漏洞”，黑客利用漏洞可以做下面的事情。

（1）获得系统信息。有些漏洞可以泄露系统信息，暴露敏感资料，从而进一步入侵系统。

（2）入侵系统。通过漏洞进入系统内部，取得服务器上的内部资料或完全掌管服务器。

（3）寻找下一个目标。一个胜利意味着下一个目标的出现，黑客会充分利用自己已经掌管的服务器作为工具，寻找并入侵下一个系统。

（4）做一些好事。正派黑客在完成上面的工作后，就会修复漏洞或者通知系统管理员，做出一些维护网络安全的事情。

（5）做一些坏事。邪派黑客在完成上面的工作后，会判断服务器是否还有利用价值。如果有利用价值，他们会在服务器上植入木马或者后门，便于下一次来访；而对没有利用价值的服务器他们决不留情，系统崩溃会让他们感到无限的快感。

1.5.3 网络攻击分类

攻击可被分为两类：主动攻击和被动攻击。

（1）主动攻击包含攻击者访问他所需信息的故意行为。比如远程登录到指定机器的 25 端口找出公司运行的邮件服务器的信息；伪造无效 IP 地址去连接服务器，使接收到错误 IP 地址的系统浪费时间去连接那个非法地址。攻击者是在主动地做一些不利于你或你的公司系统的事情。正因为如此，如果要找到他们是很容易的。主动攻击包括拒绝服务攻击、信息篡改、资源使用、欺骗等攻击方式。

（2）被动攻击主要是收集信息而不是进行访问，数据的合法用户对这种活动一点也不会觉察到。被动攻击包括嗅探、信息收集等攻击方法。

这样分类不是说主动攻击不能收集信息或被动攻击不能被用来访问系统。多数情况

下，这两种类型被联合用于入侵一个站点。但是，大多数被动攻击不一定包括可被跟踪的行为，因此更难被发现。

实际上，黑客实施一次入侵行为，为达到他的攻击目的会综合采用多种攻击手段，在不同的入侵阶段使用不同的方法。

1.5.4 常见网络攻击形式

虽然俗话说"树大招风"，但是网络攻击中的牺牲者往往是一些中小型的局域网。因为它们的网络安全的防御和反击能力都相对较差，故而在各种"江湖纷争"中，总是成为借刀杀人中的"人"或"刀"。俗话又说"知己知彼，百战百胜"，这里简单地列出常见的攻击形式，如图 1.2 所示。

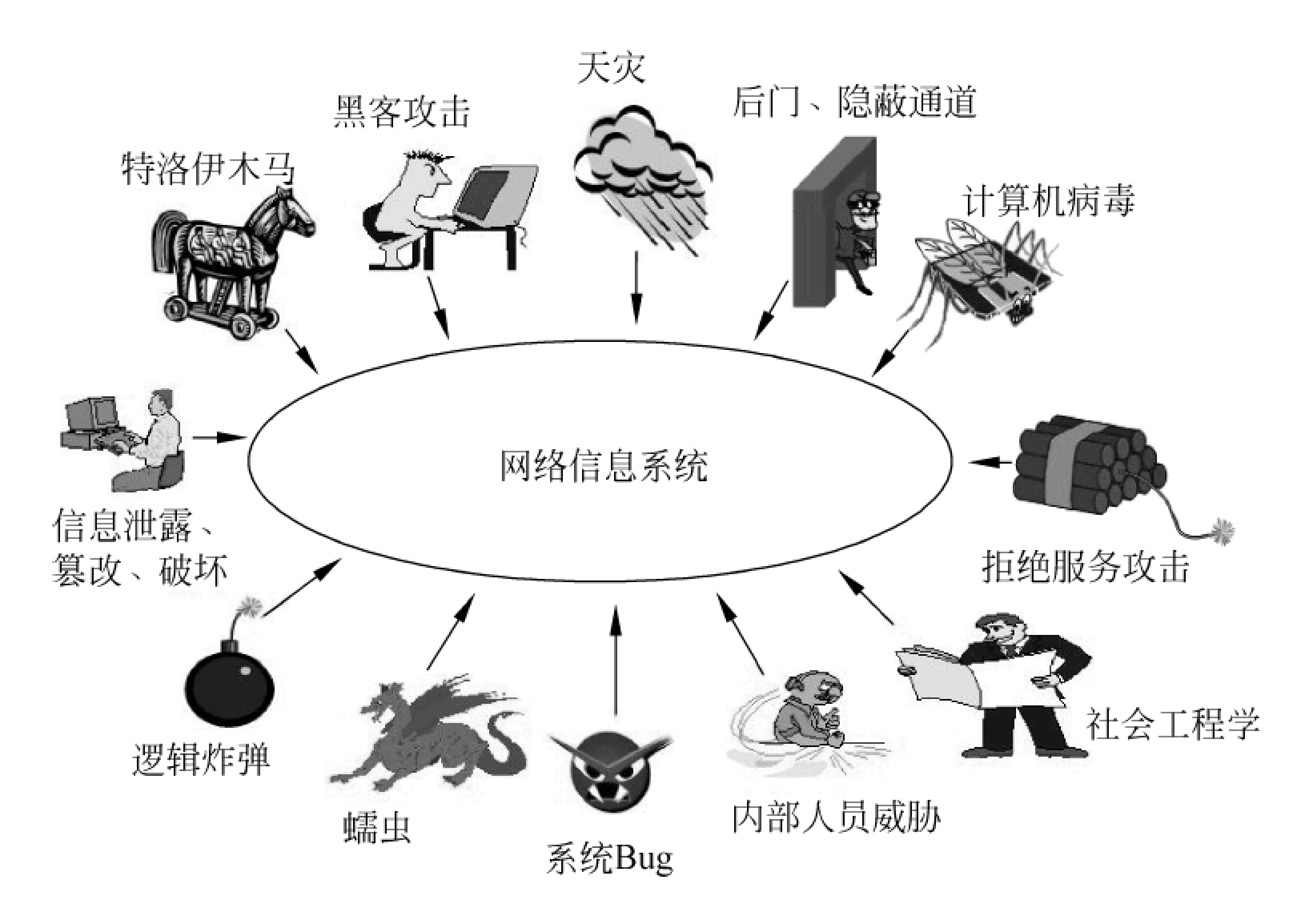


图 1.2 常见网络攻击形式

1. 逻辑炸弹

所谓"逻辑炸弹"是指在特定逻辑条件满足时，实施破坏的计算机程序。该程序触发后造成计算机数据丢失、计算机不能从硬盘或者软盘引导，甚至会使整个系统瘫痪，并出现物理损坏的虚假现象。"逻辑炸弹"引发时的症状与某些病毒的作用结果相似，并会对社会引发连带性的灾难。与病毒相比，它强调破坏作用本身，而实施破坏的程序不具有传染性。逻辑炸弹作为一种程序或任何部分的程序存在，这是冬眠，直到一个具体作品的程序逻辑被激活。这样的一个逻辑炸弹非常类似于真实世界的地雷。使用逻辑炸弹的一个经典应用是要确保支付软件使用费用。如果到某一特定日期仍然没有付款，逻辑炸弹就会激活，使软件自动删除本身。一种更恶意的形式，即逻辑炸弹会删除系统上的其他数据。

2. 系统 Bug

Bug 一词的原意是"臭虫"或"虫子"。但是现在，在计算机系统或程序中，如果隐藏着的一些未被发现的缺陷或问题，人们也叫它 Bug。所谓 Bug，是指计算机系统的硬件、系统软件(如操作系统)或应用软件(如文字处理软件)出错。硬件的出错有两个原因，一是设计错误，一是硬件部件老化失效等。

程序中隐藏的功能缺陷或错误。由于现在的软件复杂程度早已超出了一般人能控制的范围，如 Windows 操作系统会不定期地公布其中的 Bug。这些 Bug 对网络安全也会造成重大影响，如何减少以至消灭程序中的 Bug，一直是程序员所极为重视的课题。

3. 社会工程学

社会工程学是通过自然的、社会的和制度上的途径并特别强调根据现实的双向计划和设计体会来一步接一步地处理各种社会问题的学科。

黑客将社会工程定义为非计算机 Bug，通过对受害者心理弱点、本能反应、好奇心、信任、贪婪等心理陷阱进行诸如欺骗、伤害等危害手段，并最终获得信息为最终目的学科，在计算机入侵中此词条被经常使用和广泛定义。

无论是在物理上还是在虚拟的电子信息上，任何一个可以访问系统某个部分或某种服务的人都有可能构成潜在的安全风险与威胁，任何细微的信息都可能会被社会工程学使用者当做“补给资料”来运用，使其得到其他信息。这意味着如果没有把使用者与管理人员等列入到企业安全管理策略中去，将会对网络系统构成很大的安全“裂缝”。

4. 后门和隐蔽通道

事实上，没有完美无缺的代码，也许系统的某处正潜伏着重大的隐蔽通道或者后门等待人们的发现，区别只是在于谁先发现它。只要本着怀疑一切的态度，从各个方面检查所输入信息的正确性，还是可以回避这些缺陷的。比如说，如果程序有固定尺寸的缓冲区，无论是什么类型，一定要保证它不溢出；如果使用动态内存分配，一定要为内存或文件系统的耗尽做好准备，并且牢记恢复策略可能也需要内存和磁盘空间。

5. 拒绝服务攻击

拒绝服务攻击即攻击者想办法让目标机器停止提供服务或资源访问，是黑客常用的攻击手段之一。这些资源包括磁盘空间、内存、进程甚至网络带宽，从而阻止正常用户的访问。其实对网络带宽进行的消耗性攻击只是拒绝服务攻击的一小部分，只要能够对目标造成麻烦，使某些服务被暂停甚至主机死机，都属于拒绝服务攻击。拒绝服务攻击问题也一直得不到合理的解决，究其原因是由于网络协议本身的安全缺陷造成的，由此拒绝服务攻击往往成为攻击者的终极手法。攻击者进行拒绝服务攻击，实际上是让服务器实现两种效果：一是迫使服务器的缓冲区满，不接收新的请求；二是使用 IP 欺骗，迫使服务器把合法用户的连接复位，影响合法用户的连接。

6. 病毒、蠕虫和特洛伊木马

随着互联网的日益流行，各种病毒木马也猖獗起来，几乎每天都有新的病毒产生，大肆传播破坏，给广大互联网用户造成了极大的危害，几乎到了令人谈毒色变的地步。各种病毒、蠕虫、木马纷至沓来，令人防不胜防，苦恼无比。

病毒、蠕虫和特洛伊木马是导致计算机系统和计算机上的信息损坏的恶意程序。它们使网络和操作系统速度变慢，危害严重时甚至会完全破坏整个系统。它们还可使感染广为传播，在更大范围内造成危害。这三种东西都是人为编制出的恶意代码，都会对用户造成危害，人们往往将它们统称作病毒，但其实这种称法并不准确，它们之间虽然有着共性，但也有着很大的差别。详细内容见本书的第 5 章。

当然还有其他攻击方式，在这里不能一一列举，总而言之：网络之路，步步凶险。

1.6 网络安全的目标

1.6.1 第38届世界电信日主题

让全球网络更安全(Promoting Global Cyber security)。

在一个日益网络化的社会,保证网络以及信息通信技术系统和基础设施的安全,已成为当务之急。因此,必须树立对网上交易、电子商务、电子银行、远程医疗、电子政务和一系列其他应用的信心。这对于全球经济社会的未来发展至关重要。

实现网络安全取决于每个联网国家、企业和公民采取的安全措施。为防范高技能的网络犯罪分子,必须培育全球网络安全文化。这不仅需要良好的监管和立法,还需要敏于察觉威胁,并制定出基于信息通信技术的严厉对策。

1.6.2 我国网络安全的战略目标

提升网络普及水平、信息资源开发利用水平和信息安全保障水平。抓住网络技术转型的机遇,基本建成国际领先、多网融合、安全可靠的综合信息基础设施。信息安全的长效机制基本形成,国家信息安全保障体系较为完善,信息安全保障能力显著增强。这就是我国网络安全的战略目标,参见《2006—2020年国家信息化发展战略》。

1.6.3 网络安全的主要目标

通俗地说,网络安全的主要目标是保护网络信息系统,使其没有危险,不受威胁,不出事故。在这里,用五个通俗的说法来形象地描绘网络安全的目标,如图1.3所示。

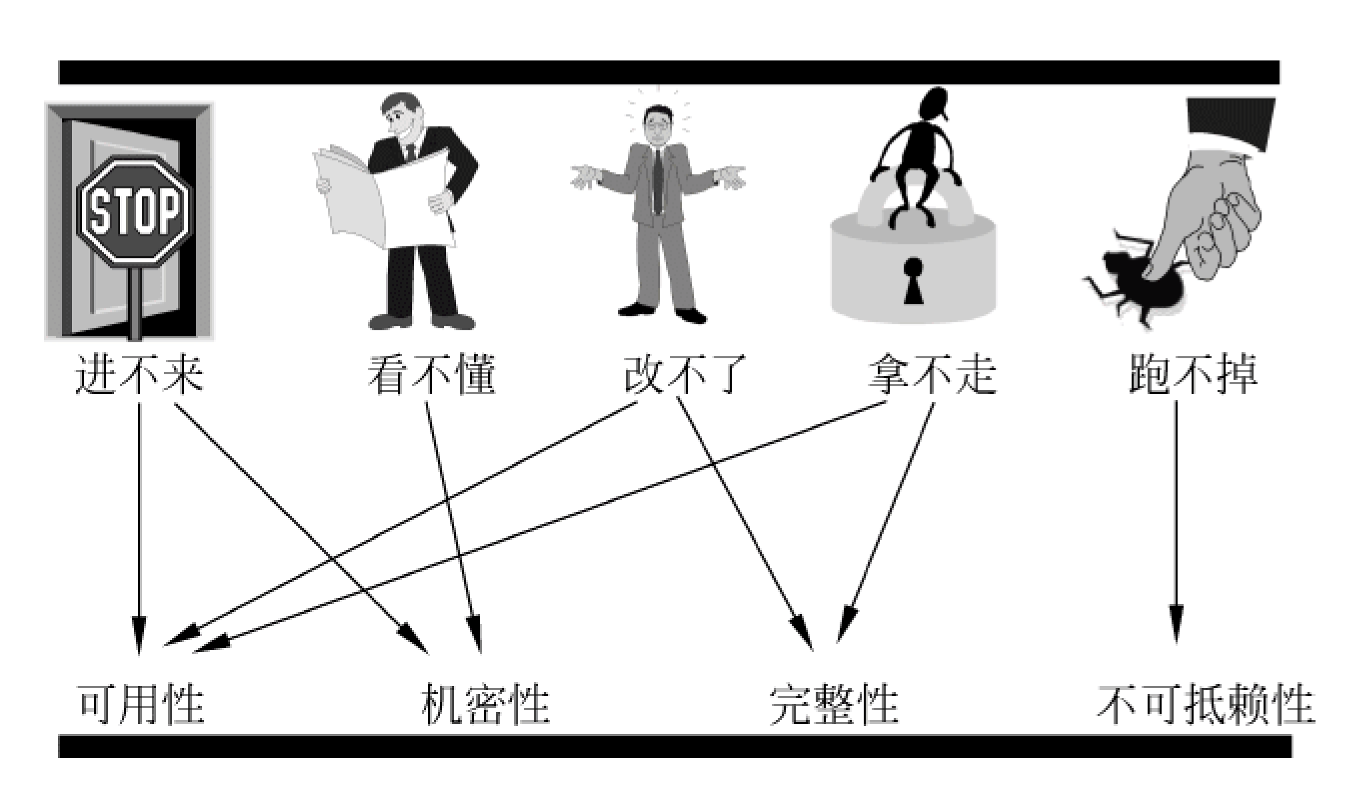


图1.3 网络安全的主要目标

可将上述说法归纳总结为以下四个方面。

1. 可用性

可用性指信息或者信息系统可被合法用户访问,并按其要求运行的特性。

如图1.3所示,“进不来”、“改不了”和“拿不走”都实现了信息系统的可用性。

人们通常采用一些技术措施或网络安全设备来实现这些目标。例如,使用防火墙,把攻击者阻挡在网络外部,让他们“进不来”。即使攻击者进入了网络内部,由于有加密机制,会使他们“改不了”和“拿不走”关键信息和资源。

2. 机密性

机密性将对敏感数据的访问权限制在那些经授权的个人，只有他们才能查看数据。机密性可防止向未经授权的个人泄露信息，或防止信息被加工。

如图1.3所示，“进不来”和“看不懂”都实现了信息系统的机密性。

人们使用口令对进入系统的用户进行身份鉴别，非法用户没有口令就“进不来”，这就保证了信息系统的机密性。即使攻击者破解了口令进入系统，加密机制也会使得他们“看不懂”关键信息。例如，甲给乙发送加密文件，只有乙通过解密才能读懂其内容，其他人看到的是乱码。由此便实现了信息的机密性。

3. 完整性

完整性指防止数据未经授权或意外改动，包括数据插入、删除和修改等。为了确保数据的完整性，系统必须能够检测出未经授权的数据修改。其目标是使数据的接收方能够证实数据没有被改动过。

如图1.3所示，“改不了”和“拿不走”都实现了信息系统的完整性。

使用加密机制，可以保证信息系统的完整性，攻击者无法对加密信息进行修改或者复制。完整性与机密性不同，机密性要求信息不被泄露给未授权的人，而完整性则要求信息不能受到各种原因的任意破坏。

4. 不可抵赖性

不可抵赖性也叫不可否认性，即防止个人否认先前已执行的动作，其目标是确保数据的接收方能够确信发送方的身份。例如，接收者不能否认收到消息，发送者也不能否认发送过消息。

如图1.3所示，“跑不掉”就实现了信息系统的不可抵赖性。

如果攻击者进行了非法操作，系统管理员使用审计机制或签名机制也可让他们无处遁形。

网络安全的技术主要包括监控、扫描、检测、加密、认证、防攻击、防病毒以及审计等几个方面，其中加密技术是核心技术，已经渗透到大部分安全产品之中，并正向芯片化方向发展。

课 后 习 题

选择题

1. 向有限的空间输入超长的字符串是(　　)攻击手段。

A. 缓冲区溢出　　B. 网络监听　　C. 端口扫描　　D. IP欺骗

2. 使网络服务器中充斥着大量要求回复的信息，消耗带宽，导致网络或系统停止正常服务，这属于(　　)漏洞。

A. 拒绝服务　　B. 文件共享　　C. BIND漏洞　　D. 远程过程调用

3. 不属于黑客被动攻击的是(　　)。

A. 缓冲区溢出　　B. 运行恶意软件

C. 浏览恶意代码网页　　D. 打开病毒附件

4. 抵御电子邮箱入侵措施中，不正确的是(　　)。

A. 不用生日做密码　　B. 不要使用少于5位的密码

C. 不要使用纯数字　　D. 自己做服务器

5. 不属于常见的危险密码的是(　　)。

A. 跟用户名相同的密码　　B. 使用生日作为密码

C. 只有4位数的密码　　D. 10位的综合型密码

6. 属于黑客入侵的常用手段的是(　　)。

A. 口令设置　　B. 邮件群发　　C. 窃取情报　　D. IP欺骗

7. 计算机网络系统的安全威胁不包括(　　)。

A. 黑客攻击　　B. 网络内部的安全威胁

C. 病毒攻击　　D. 自然灾害

8. 信息安全危害的两大源头是病毒和黑客,因为黑客是(　　)。

A. 计算机编程高手　　B. Cookies的发布者

C. 网络的非法入侵者　　D. 信息垃圾的制造者

9. 以下不属于计算机安全措施的是(　　)。

A. 下载并安装系统漏洞补丁程序　　B. 安装并定时升级正版杀毒软件

C. 安装软件防火墙　　D. 不将计算机连入互联网

10. 为了降低风险,不建议使用的Internet服务是(　　)。

A. Web服务　　B. 外部访问内部系统

C. 内部访问Internet　　D. FTP服务

11. 截至2008年6月底,中国网民数量达到(　　),网民规模跃居世界第一位。

A. 2.53亿　　B. 3.53亿　　C. 0.53亿　　D. 1.53亿

填空题

1. 比较常用的防范黑客的技术产品有(　　)、(　　)和安全工具包/软件。

2. 用户的密码按照时间或使用次数不断动态变化,每个密码只使用一次,这种密码叫做(　　)。

3. 生物特征识别技术指通过计算机,利用人体所固有的生理特征或行为特征来进行个人身份鉴定。常用的生物特征包括指纹、掌纹、(　　)、(　　)、(　　)、脸像等。

4. (　　)是特指计算机系统的非法侵入者。

5. 网络攻击可被分为两类:(　　)和(　　)。

6. (　　)即攻击者想办法让目标机器停止提供服务或资源访问,是黑客常用的攻击手段之一。

简答题

1. 造成网络不安全的主要原因有哪些?

2. 威胁企业安全的网络危险行为有哪些?

3. 防范钓鱼网站的方法是什么?

4. 简述网络密码的重要性。有哪几种方法可以保护密码不被破解或者被盗取?

5. 黑客的行为主要有哪些?

6. 网络攻击技术主要包括哪些方面?

7. 常见的网络攻击形式有哪些?

8. 我国网络安全的战略目标是什么?

9. 网络安全的目标可归纳为哪四个方面?

第2章 网络监控软件原理

2.1 网络监控软件介绍

计算机网络的普及应用已渗透到社会各个层面，网络给各行各业带来便利的同时也带来了安全和管理问题。互联网是一把双刃剑，有了网络，实现网络办公的同时，企业员工利用工作时间在网上看新闻、玩游戏、干私活、聊天、泄密公司资料、炒股票、下电影、听歌曲、浏览色情站点甚至利用公司的网络为自己找工作。大量消耗了公司的资源，影响工作效率、泄露企业机密甚至丢失客户资源，令人痛心。利用局域网网络监控软件这一行之有效的辅助管理手段，并结合企业的内部管理机制对企业信息进行管理以预防和避免上述事件的发生，能达到事半功倍的效果，这一方法，已经为大家所认知。

2.1.1 为什么要使用网络监控软件

很多单位很舍得对网络以及计算机设备的投入，但却不舍得对应用软件特别是安全软件的投入；组建了性能出色的网络环境以及购买了现代化的办公设备，这些高端设备却成了浪费公司人力和财力，甚至是纵容员工上班时间做单位之外的事情的“帮凶”，不仅降低了工作效率，甚至会造成更大的损失。设置网络监控管理，防患于未然，变得尤为必要。

目前很多企业配备了专门的网络管理人员管理企业所构建的网站，虽然管好了设备，但设备所带来的方便却降低了企业员工的工作效率（都用网络干别的事情去了），加大了商业信息泄露的风险（因为缺乏管理，客户资料很可能被自己人传送给竞争对手，成为对方的资源）。因此，企业内部网络的管理仅仅靠购买设备是不够的，仅仅建设网站也是不够的，只管理网络设备还是不够的，还需要把员工使用网络的内容做监控，把使用网络的行为管理起来。尤其是外贸企业、技术研发类企业（如软件开发、机械工程）、政府机关、银行、医院、部队等关键任务机构，对员工的上网监督管理必不可少。

2.1.2 网络监控软件主要目标

网络监控系统总体目标是能有效防止员工通过网络以各种方式泄密，防止并追查重要资料、机密文件的外泄渠道，实现对网络计算机及网络资源的统一管理和有效监控。监督、审查、限制、规范网络使用行为，未经授权不得以任何方式外发文件、不得在上班时间利用网络做不应该做的事（例如，聊天、游戏、外发资料、BT 恶性下载和股票等），能够记录网络往来的内容（比如外贸企业的订单过程、QQ/MSN 聊天记录内容和行为过程），对计算机的各种端口和设备实施全面管理和控制，对使用计算机、上网、收发邮件、网上聊天和计算机游戏进行严格管理，能够进行流量限制以及网站访问统计，分析员工使用网络情况等。

2.1.3 网络监控软件的分类

按照运行原理区分为监听模式和网关模式两种。

1. 监听模式

通过抓取总线 MAC 层数据帧方式而获得监听数据，并利用网络通信协议原理而实现控制的方法。采用如下方法之一来解决安装问题：

1）通过共享式 hub（集线器）

这个模式是一个比较通用的方法，但由于 hub 基本都是 10MB 的，因此在网络性能上将有很大限制，也意味着有丢包的危险。目前 hub 几乎到了淘汰的边缘，也不适合大型网络环境，因此有很大局限。

2）通过镜像交换机

由于网管的镜像交换机价格相对较贵并需要专业的配置，所以中小企业并没有带镜像功能的交换机；如果规模比较小（比如 30 台计算机以下），那么添置镜像交换机就意味着成本的提高；有些便宜的交换机虽然带镜像功能，但在镜像后由于双向（监视和控制）数据流处理不完善而导致交换机瞬间阻塞现象。但相比 hub 模式来说，使用镜像交换机实现监听无疑是理想的选择。

3）通过代理/网关服务器

代理/网关服务器，就是在服务器上通过 Windows 连接共享设置，其他计算机通过这个代理/网关服务器分享上网。一般都是双网卡模式：一个网卡连接外网，另外一个网卡连接内网。但现在大部分的网络已经不再使用这个模式，直接通过路由的 NAT 上网共享模式。

从上面文字的描述中可以看到，其实所有的监听模式的解决方法都是不太可靠的，而目前所有使用 WINPCAP 驱动的网络监控软件以及使用网络层驱动的软件都是监听模式。如果一个软件要求使用前面的三个安装方法之一，那就肯定是监听模式软件，因此真正商业运行的话强烈建议网关模式。

2. 网关模式

由于所有出口数据流都必须经过该网关，因此控制方面可以说是最强大、完美而无任何副作用的方式。网关模式克服了目前所有的采用 WINPCAP 模式或网络层驱动模式下的所有弱点，克服了所有监听模式下阻断 UDP 的致命弱点，是网络监控最理想的模式。

网关模式按照管理目标区分为内网监控和外网监控两种。

(1) 内网监控的主要目标是管理网内计算机的所有资源和使用过程，比如网内的计算机硬件资源（有什么设备、是否允许使用）、软件资源（安装了什么软件、是否允许使用）、数据资源（有什么重要资料文件、数据，是否被合法使用）、行为操作（对工作的评估、使用计算机的合法性、干了一些什么事情），等等。

(2) 外网监控的主要目标是监视网内计算机的上网内容和管理上网行为，比如网络监控、邮件监控、上网监控、网页监控、FTP 监控、MSN 聊天内容监控、游戏监控、流量监控和限制 QQ/MSN 等聊天行为监控、自定义监控、TCP/UDP 全系列双向端口监视和控制、BT 完美禁止，等等。

无论是硬件还是软件方式的解决方法，都应包含内网监控和外网监控产品，通过合理的

投资组合获得不断升级,更新对资源和行为的管理。硬件在性能上相比软件来说较为优势,但在拓展性、升级更新、投资成本上却会造成很大的麻烦。

2.2 Sniffer 工具介绍

2.2.1 Sniffer 的原理

Sniffer 程序是一种利用以太网的特性把网络适配卡(NIC)置为混杂(promiscuous)模式状态的工具,一旦网卡设置为这种模式,它就能接收传输在网络上的每一个信息包。

通常情况下,网卡只接收和自己的地址有关的信息包,即传输到本地主机的信息包。要使 Sniffer 能接收并处理这种方式的信息,系统需要支持 BPF(作用是获得在数据链路层上的所有数据),Linux 下需要支持 SOCKET-PACKET。但一般情况下,网络硬件和 TCP/IP 堆栈不支持接收或者发送与本地计算机无关的数据包,所以,为了绕过标准的 TCP/IP 堆栈,网卡就必须设置为混杂模式。一般情况下,要激活这种方式,内核必须支持这种伪设备 Bpfilter,而且需要管理员权限来运行这种程序。所以,Sniffer 需要以管理员身份安装。如果只是以本地用户的身份进入了系统,那么不可能嗅探到管理员的密码,所以不能运行 Sniffer。

也有基于无线网络、广域网络(DDN、FR)甚至光网络(POS、Fiber Channel)的监听技术,这时候略微不同于以太网络上的捕获概念,其中通常会引入 TAP(测试介入点)这类的硬件设备来进行数据采集。因为不是十分常见,所以也不再详细介绍。

2.2.2 Sniffer 的分类

Sniffer 分为软件和硬件两种。软件的 Sniffer 有 Sniffer Pro、Network Monitor、PacketBone 等,其优点是易于安装部署,易于学习使用,同时也易于交流;缺点是无法抓取网络上所有的传输,某些情况下也就无法真正了解网络的故障和运行情况。硬件的 Sniffer 通常称为协议分析仪,一般都是商业性的,价格也比较昂贵,但会具备支持各类扩展的链路捕获能力以及高性能的数据实时捕获分析的功能。

基于以太网络嗅探的 Sniffer 只能抓取一个物理网段内的包,就是说,你和监听的目标中间不能有路由或其他屏蔽广播包的设备,这一点很重要。所以,对一般拨号上网的用户来说,是不可能利用 Sniffer 来窃听到其他人的通信内容的。

2.2.3 网络监听的目的

当一个黑客成功地攻陷了一台主机,并拿到了管理员权限,而且还想利用这台主机去攻击同一(物理)网段上的其他主机时,他就会在这台主机上安装 Sniffer 软件,对以太网设备上传送的数据包进行侦听,从而发现感兴趣的包。如果发现符合条件的包,就把它存到一个 Log 文件中去。通常设置的这些条件是包含字 username 或 password 的包,这样的包里面通常有黑客感兴趣的密码之类的东西。一旦黑客截获了某台主机的密码,就会立刻进入这台主机。

如果 Sniffer 运行在路由器上或有路由功能的主机上,就能对大量的数据进行监控,因

为所有进出网络的数据包都要经过路由器。

Sniffer 属于第 M 层次的攻击。也就是说，只有在攻击者已经进入了目标系统的情况下，才能使用 Sniffer 这种攻击手段，以便得到更多的信息。

Sniffer 除了能得到口令或用户名外，还能得到更多的其他信息，比如一段保密信息、在网上传送的金融信息等。Sniffer 几乎能得到任何在以太网上传送的数据包。

2.2.4 Sniffer 的应用

Sniffer 在当前网络技术中应用得非常广泛。Sniffer 既可以作为网络故障的诊断工具，也可以作为黑客嗅探和监听的工具。最近两年，网络监听技术出现了新的重要特征。传统的 Sniffer 技术是被动地监听网络通信、用户名和口令；而新的 Sniffer 技术出现了主动地控制通信数据的特点，把 Sniffer 技术扩展到了一个新的领域。Sniffer 主要有以下几个方面的应用：

(1) Sniffer 可以帮助评估业务运行状态。如果网管能告诉老板说，公司的业务运行正常，性能良好，比起跟老板报告说网络没有问题，我想老板会更愿意听前面的报告，但要做这样的报告，光说是不行的，必须有根据，Sniffer 就能提供这样的根据。比如各个应用的响应时间，一个操作需要的时间，应用带宽的消耗，应用的行为特征，应用性能的瓶颈等，这些 Sniffer 都可以提供相应的数据。

(2) Sniffer 能够帮助评估网络的性能。比如各链路的使用率，网络的性能趋势，网络中哪一些应用消耗带宽最多，网络上哪一些用户消耗带宽最多，各分支机构流量状况，影响网络性能的主要因素，可否做一些相应的控制等。

(3) Sniffer 帮助快速定位故障。Sniffer 的三大功能：监测、专家系统、解码都可以帮助快速定位故障。

(4) Sniffer 可以帮助排除潜在的威胁。网络中有各种各样的应用，有一些是关键应用，有一些是办公软件，有一些是业务应用，还有一些就是威胁，威胁不但对业务没有帮助，还可能带来危害，比如病毒、木马、扫描等，Sniffer 可以快速地发现它们，并且发现攻击的来源，这就为网管员做控制提供了根据。比如在 2003 年冲击波发作的时候，很多 Sniffer 的用户通过 Sniffer 快速定位受感染的机器。

(5) Sniffer 可以做流量的趋势分析。通过长期监控，可以发现网络流量的发展趋势，为将来网络改造提供建议和依据。

(6) Sniffer 可以做应用性能预测。Sniffer 能够根据捕获的流量分析一个应用的行为特征，还可以用 Sniffer 来评估应用的瓶颈在哪，不同应用瓶颈不同，Sniffer 能比较准确地预测出具体的位置。

2.2.5 Sniffer 的工作原理

通常在同一个网段的所有网络接口都有访问在物理媒体上传输的所有数据的能力，而每个网络接口都有一个硬件地址，该硬件地址不同于网络中存在的其他网络接口的硬件地址；每个网络至少还要一个广播地址(代表所有的接口地址)。在正常情况下，一个合法的网络接口应该只响应这样的两种数据帧：

(1) 帧的目标区域具有和本地网络接口相匹配的硬件地址。

（2）帧的目标区域具有“广播地址”。

在接收到上面两种情况的数据包时，网卡通过 CPU 产生一个硬件中断，该中断能引起操作系统注意，然后将帧中所包含的数据传送给系统进一步处理。

而 Sniffer 就是一种能将本地网卡状态设成混杂状态的软件，当网卡处于这种“混杂”模式时，该网卡具备“广播地址”，它对所有遭遇到的每一个帧都产生一个硬件中断以便提醒操作系统处理流经该物理媒体上的每一个报文包（绝大多数的网卡具备置成混杂方式的能力）。

可见，Sniffer 工作在网络环境中的底层，它会拦截所有正在网络上传送的数据，并且通过相应的软件处理，可以实时分析这些数据的内容，进而分析所处的网络状态和整体布局。值得注意的是，Sniffer 是极其安静的，它是一种消极的安全攻击。

通常 Sniffer 所要关心的内容可以分成以下几类。

（1）口令。这是绝大多数非法使用 Sniffer 的原因，Sniffer 可以记录到明文传送的 userid 和 passwd。即使在网络传送过程中使用了加密的数据，Sniffer 的记录一样有可能使入侵者使用破解软件来恢复加密数据。

（2）金融账号。许多用户很放心在网上使用自己的信用卡或现金账号，然而 Sniffer 可以很轻松地截获在网上传送的用户姓名、口令、信用卡号码、截止日期、账号和 pin。

（3）偷窥机密或敏感的信息数据。通过拦截数据包，入侵者可以很方便地记录别人之间敏感的信息传送，或者干脆拦截整个的 E-mail 会话过程。

（4）窥探低级的协议信息。通过对底层的信息协议记录，比如记录两台主机之间的网络接口地址、远程网络接口 IP 地址、IP 路由信息和 TCP 连接的字节顺序号码等。这些信息由非法入侵的人掌握后将对网络安全构成极大的危害，通常有人用 Sniffer 收集这些信息只有一个原因：他正在进行一次欺诈（通常的 IP 地址欺诈就要求你准确插入 TCP 连接的字节顺序号）。

2.3　Sniffer 的工作环境

Sniffer 的正当用处在于分析网络的流量，以便找出所关心的网络中潜在的问题。例如网络的某一段运行得不是很好，报文的发送比较慢，而用户又不知道问题出在什么地方，此时就可以用 Sniffer 来做出精确的问题判断。

Sniffer 在功能和设计方面有很多不同。有些只能分析一种协议，而另一些可能能够分析几百种协议。一般情况下，大多数的 Sniffer 至少能够分析标准以太网、TCP/IP、IPX 和 DECNet 等协议。

Sniffer 通常是软硬件的结合。专用的 Sniffer 价格非常昂贵。另一方面，免费的虽然不需要花什么钱，但得不到什么技术支持。

Sniffer 与一般的键盘捕获程序不同。键盘捕获程序捕获在终端上输入的键值，而 Sniffer 则捕获真实的网络报文。数据在网络上是以很小的称为帧（Frame）的单位传输的，帧由好几部分组成，不同的部分执行不同的功能（例如，以太网的前 12 个字节存放的是源和目的地址，这些字节表明了数据的来源和去处。以太网帧的其他部分存放实际的用户数据、TCP/IP 的报文头或 IPX 报文头等）。

帧通过特定的称为网络驱动程序的软件进行成型，然后通过网卡发送到网线上。通过网线到达它们的目的机器，在目的机器的一端执行相反的过程。接收端机器的以太网卡捕获到这些帧，并告诉操作系统帧的到达，然后对其进行存储。就是在这个传输和接收的过程中，Sniffer 会造成安全方面的问题。

每一个在 LAN 上的工作站都有其硬件地址。这些地址唯一地表示着网络上的机器（这一点与 Internet 地址系统比较相似）。当用户发送一个报文时，这些报文就会发送到 LAN 上所有可用的机器。

在一般情况下，网络上所有的机器都可以“听”到通过的流量，但对不属于自己的报文则不予响应（换句话说，工作站 A 不会捕获属于工作站 B 的数据，而是简单地忽略这些数据）。

如果在工作站的网络接口处于混杂模式，那么它就可以捕获网络上所有的报文和帧，如果一个工作站被配置成这样的方式，它就是一个 Sniffer。事实上，如果在网络上存在非授权的 Sniffer 就意味着系统已经暴露在别人面前了。

一般只嗅探每个报文的前 200～300 个字节。用户名和口令都包含在这一部分中，这是我们关心的真正部分。也可以嗅探给定接口上的所有报文，如果有足够的空间进行存储，有足够的能力进行处理的话，将会发现另一些非常有用的数据。

简单地放置一个 Sniffer，将其放到随便什么地方将不会起到什么作用。将 Sniffer 放置于被攻击机器或网络附近，这样将捕获到很多口令，还有一个比较好的方法就是放在网关上。如果这样的话就能捕获网络和其他网络进行身份鉴别的过程。这样的方式将成倍地增加可用数据。

2.4　Sniffer Pro 软件使用

Sniffer Pro 是美国 Network Associates 公司出品的一款网络分析软件。它可用于网络故障分析与性能管理，在网络界应用非常广泛。

通过 Sniffer Pro 实时监控，及时发现网络环境中的故障（例如病毒、攻击、流量超限等非正常行为）。对于很多企业、网吧网络环境中，网关（路由、代理等）自身不具备流量监控、查询功能，本文将是一个很好的解决方案。Sniffer Pro 强大的实用功能还包括网内任意终端流量实时查询、网内终端与终端之间流量实时查询、终端流量 TOP 排行、异常告警等。同时，将数据包捕获后，通过 Sniffer Pro 的专家分析系统帮助用户更进一步分析数据包，以便更好地分析、解决网络异常问题。

（1）部署 Sniffer pro 软件，如图 2.1 所示的拓扑。

（2）配置交换机端口镜像。端口镜像就是把交换机一个或多个端口（VLAN）的数据镜像到一个或多个端口的方法。交换机的工作原理与 hub 有很大的不同，hub 组建的网络数据交换都是通过广播方式进行的，而交换机组建的网络是根据交换机内部 MAC 表（通常也称 IP-MAC 表）进行数据转发，因此需要通过配置交换机来把一个或多个端口（VLAN）的数据转发到某一个端口来实现对网络的监听。

（3）Sniffer Pro 安装、启动、配置（详见第 10 章）。

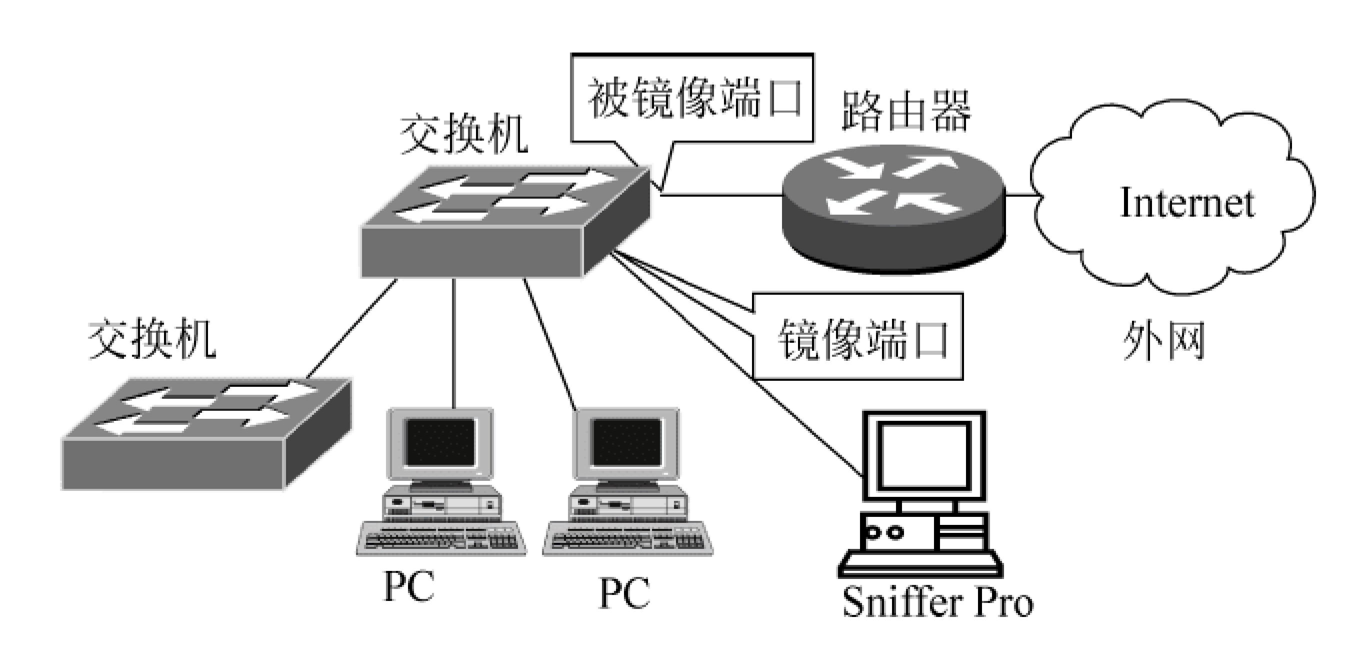


图 2.1　带有 Sniffer pro 的网络拓扑

2.6　网路岗工具介绍

2.6.1　网路岗的基本功能

网路岗软件通过旁路对网络数据流进行采集、分析和识别，实时监视网络系统的运行状态，记录网络事件、发现安全隐患，并对网络活动的相关信息进行存储、分析和协议还原。该产品可监视企业内部员工是否将公司机密资料通过因特网外传到竞争对手的手中。

网路岗软件可以监控的内容包括监控邮件内容和附件(包括 Web 邮件监控)、监控聊天内容、监控上网网站、监控 FTP 外传文件、监控 Telnet 命令、监控上网流量，IP 过滤、端口过滤、网页过滤、封堵聊天游戏，限制外发资料邮件大小，限制网络流量，IP-MAC 绑定，截取屏幕等。

2.6.2　网路岗对上网的监控能做到什么程度

(1) 让某人只能在规定时间上网，且只能上指定的网站。

(2) 让某人只能在哪个网站上收发邮件，只能收发哪类的邮箱。

(3) 谁什么时候通过什么软件发送了什么邮件或通过哪个网站发了什么软件，邮件的内容和附件是什么，以及附件在发送者计算机的具体位置。

(4) 规定某人只能发送多大的邮件。

(5) 规定某人只能发送到哪些目标邮箱。

(6) 轻松抓取指定人的计算机屏幕。

(7) 所有机器在一天内各时间段的上网流量。

(8) 某台机器哪些外部端口不能用，或只能通过哪些端口和外界联系，等等。

2.6.3　网路岗安装方式

(1) 网路岗安装在代理服务器上，通过安装“代理服务器软件”或“网路岗 NAT”，实现所有机器共享一个出口上网，如图 2.2 所示的拓扑。

安装方法：将网路岗安装在代理服务器上，绑定内网的网卡，网路岗设置为“非旁路监控”模式，重新启动计算机。

(2) 网路岗安装在 hub 的一个端口上，通过“IP 分享器、路由器或防火墙”实现整个网

络共享一个出口上网，且内部交换机均不具备设置镜像端口的功能，如图 2.3 所示。

图 2.2　网路岗在代理服务器上的安装拓扑

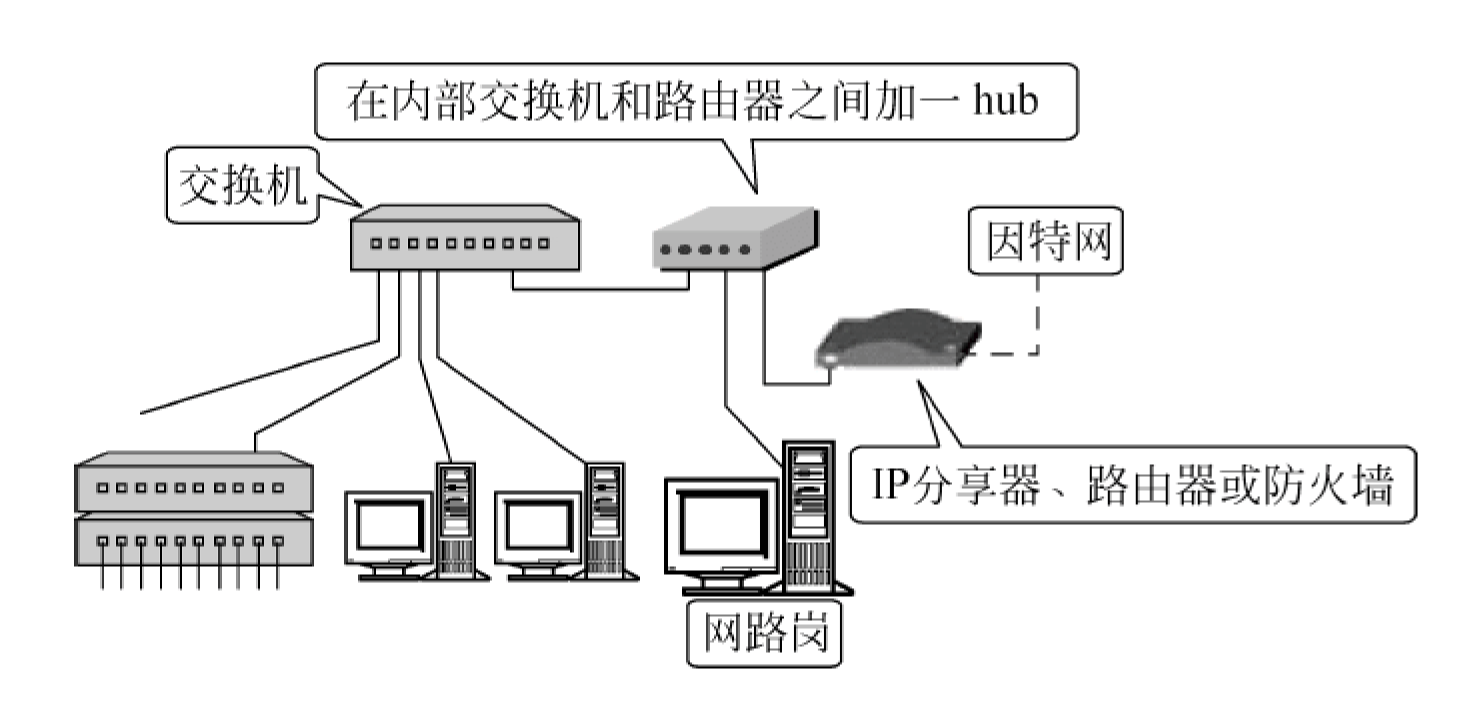


图 2.3　网路岗在 hub 的一个端口上的安装拓扑

安装方法：在内部交换机和路由器之间加一共享式 hub，再将安装网路岗的机器网线也接入到 hub 上，网路岗设置为“旁路监控”模式。

(3) 网路岗安装在交换机的镜像端口上，通过“IP 分享器、路由器或防火墙”实现整个网络共享一个出口上网，且内部主交换机具备设置镜像端口的功能，如图 2.4 所示。

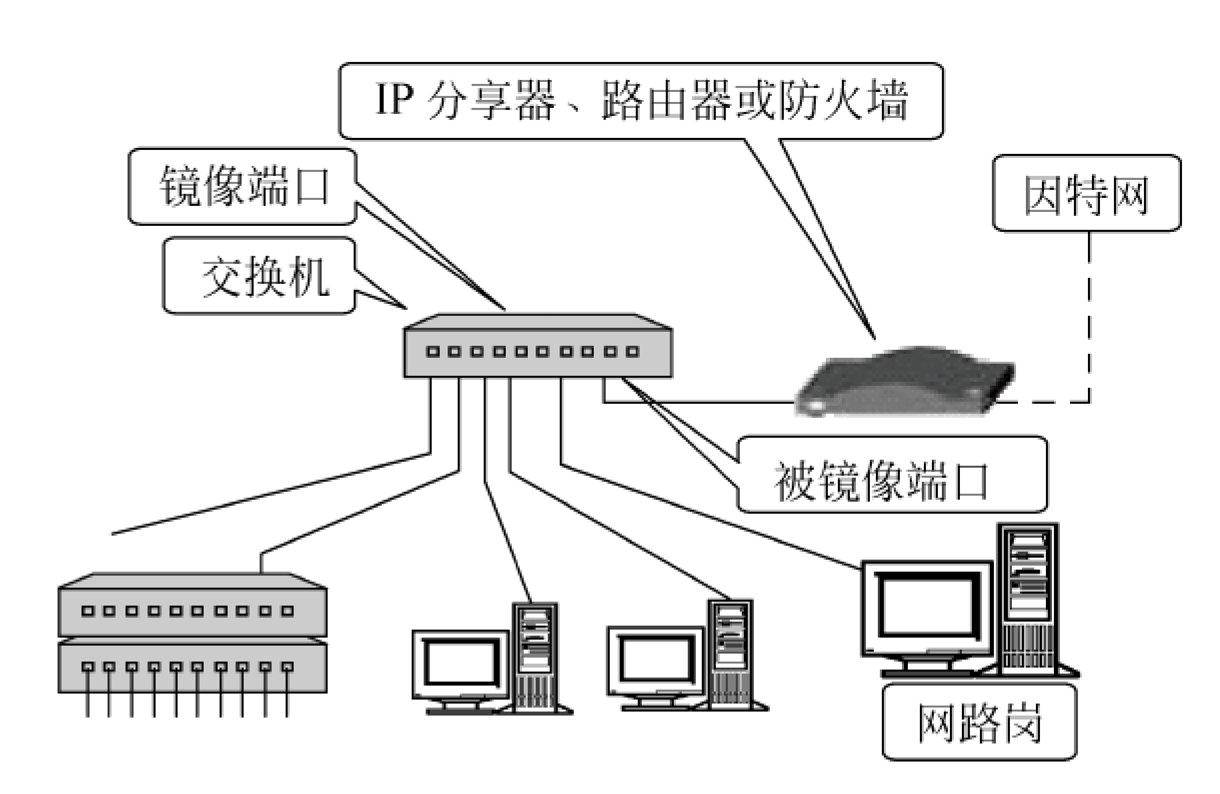


图 2.4　网路岗在交换机的镜像端口上的安装拓扑

安装方法：在内部主交换机上设置端口镜像，将接路由器的网线设置为“被镜像端口”，将接网路岗的网线设置为“镜像端口”。网路岗设置为“旁路监控”模式。

(4) 网路岗安装在网络桥上，在一台双网卡计算机上建立“网络”，将该“网络桥”放在 Internet 出口处，如图 2.5 所示的拓扑。

安装方法：直接将“网路岗”安装在启用“网络桥”的机器上，“网路岗”绑定在内网的网

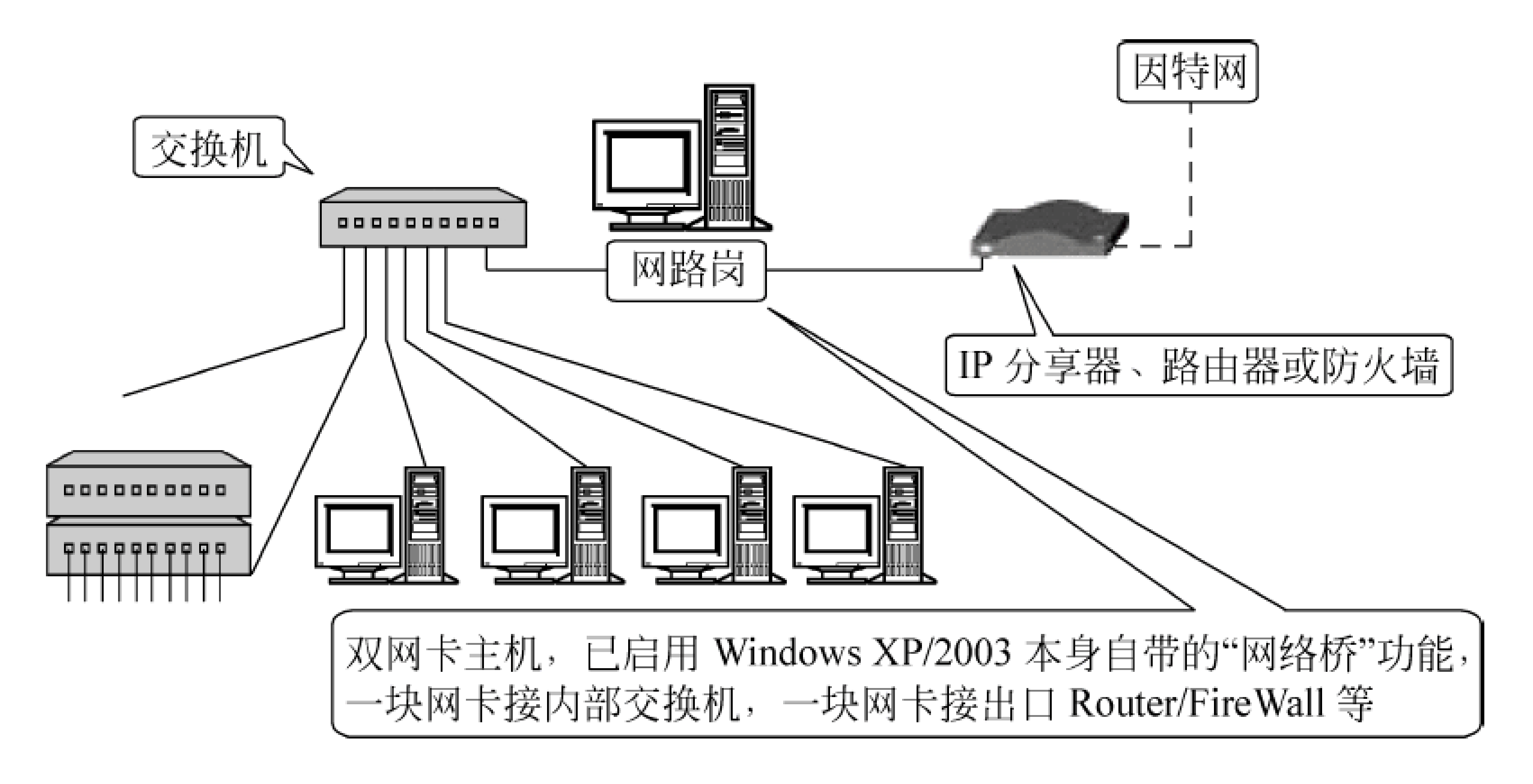


图 2.5　网路岗在网络桥上的安装拓扑

卡上，同时给“网络桥”配置 IP 以使其能访问内部网其他机器。网路岗设置为“非旁路监控”模式，重新启动计算机。

(5) 网路岗安装、启动、配置 、使用(详见第 11 章)。

课 后 习 题

填空题

1. 内网监控的主要目标是管理网内计算机的(　　)和(　　)。
2. 外网监控的主要目标是监视网内计算机的(　　)和管理(　　)。
3. 大多数的嗅探器至少能够分析标准以太网、(　　)、(　　)、DECNet 等协议。
4. 网络监控软件按照运行原理区分为(　　)和(　　)两种类型。

简答题

1. 什么叫数据包监测？它有什么作用？
2. 网络监控软件主要目标有哪些？
3. 网络监控软件的解决方案有哪些分类？
4. Sniffer 的工作原理是什么？
5. Sniffer 所要关心的内容可以分成哪几类？
6. Sniffer 主要有哪几个方面的应用？
7. 什么是端口镜像？为什么需要端口镜像？
8. 网路岗软件的基本功能有哪些？
9. 网路岗软件有哪几种安装方式？

第3章 操作系统安全

3.1 国际安全评价标准的发展及其联系

计算机系统安全评价标准是一种技术性法规。在信息安全这一特殊领域，如果没有这一标准，与此相关的立法、执法就会有失偏颇，最终会给国家的信息安全带来严重后果。由于信息安全产品和系统的安全评价事关国家的安全利益，因此许多国家都在充分借鉴国际标准的前提下，积极制订本国的计算机安全评价认证标准。

第一个有关信息技术安全评价的标准诞生于20世纪80年代的美国，就是著名的《可信计算机系统评价准则》(Trusted Computer System Evaluation Criteri，TCSEC，又称桔皮书)。该准则对计算机操作系统的安全性规定了不同的等级。从20世纪90年代开始，一些国家和国际组织相继提出了新的安全评价准则。1991年，欧共体发布了《信息技术安全评价准则》(Information Technology Security Evaluation Criteria，ITSEC)。1993年，加拿大发布了《加拿大可信计算机产品评价准则》(Canadian Trusted Computer Product Evaluation Criteria，CTCPEC)，CTCPEC综合了TCSEC和ITSEC两个准则的优点。同年，美国在对TCSEC进行修改补充并吸收ITSEC优点的基础上，发布了《信息技术安全评价联邦准则》(FC)，参见图3.1。

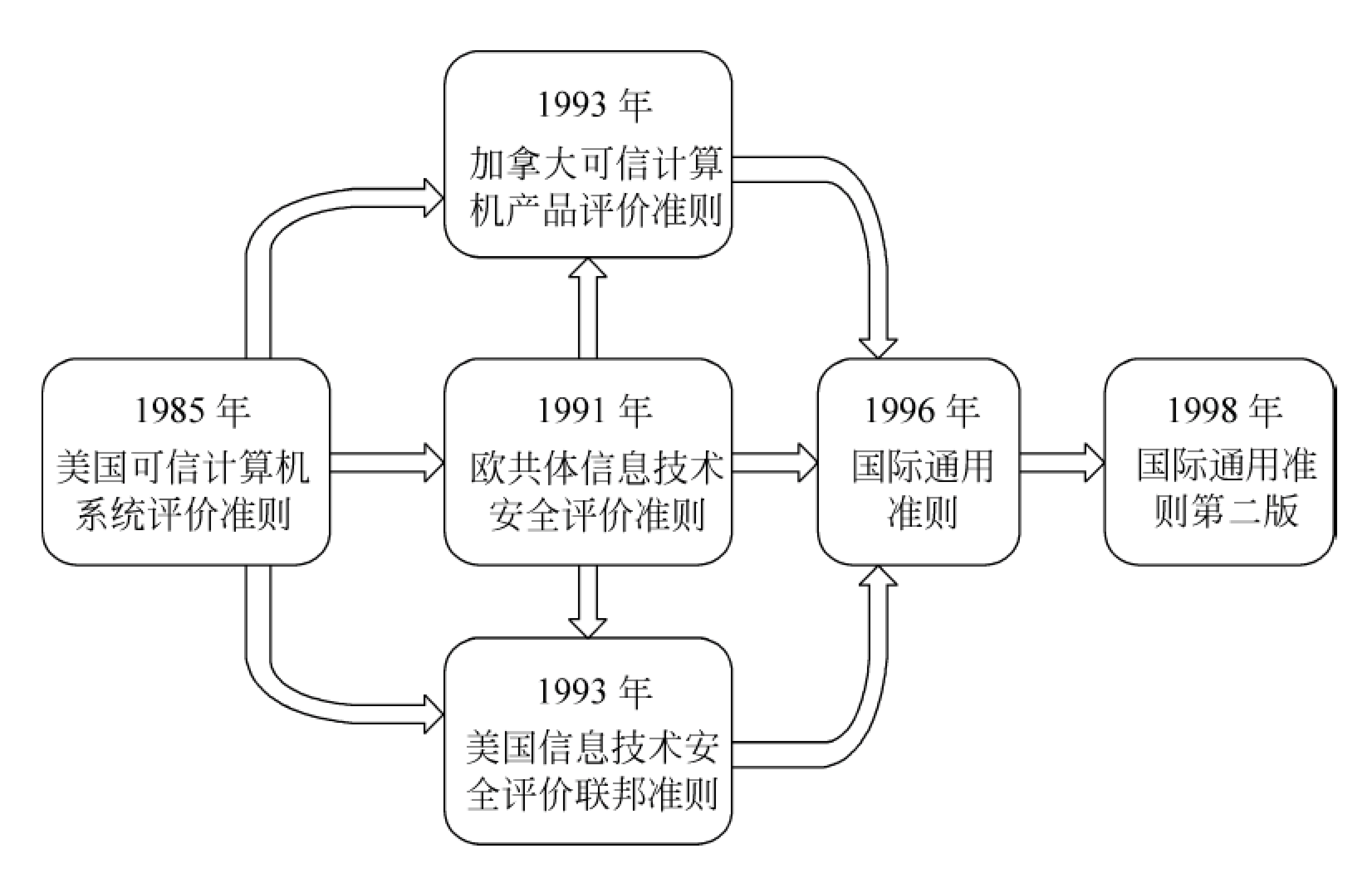


图 3.1　安全评价标准的发展

1996年6月，上述国家共同起草了一份通用准则(CC)，并将CC推广为国际标准。CC发布的目的是建立一个各国都能接受的通用的安全评价准则，国家与国家之间可以通过签订

互认协议来决定相互接受的认可级别，这样能使基础性安全产品在通过 CC 准则评价并得到许可进入国际市场时，不需要再作评价。此外，国际标准化组织和国际电工委也已经制定了上百项安全标准，其中包括专门针对银行业务制定的信息安全标准。国际电信联盟和欧洲计算机制造商协会也推出了许多安全标准。

3.1.1 计算机安全评价标准

计算机安全评价标准——TCSEC 是计算机系统安全评估的第一个正式标准，具有划时代的意义。该准则于 1970 年由美国国防科学委员会提出，并于 1985 年 12 月由美国国防部公布。TCSEC 最初只是军用标准，后来延至民用领域。TCSEC 将计算机系统的安全划分为 4 个等级 7 个级别。

D 类安全等级：D 类安全等级只包括 D1 一个级别。D1 的安全等级最低，D1 系统只为文件和用户提供安全保护。D1 系统最普通的形式是本地操作系统，或者是一个完全没有保护的网络。

C 类安全等级：该类安全等级能够提供审慎的保护，并为用户的行动和责任提供审计能力。C 类安全等级可划分为 C1 和 C2 两类。C1 系统的可信任运算基础体制，通过将用户和数据分开来达到安全的目的。在 C1 系统中，所有的用户以同样的灵敏度来处理数据，即用户认为 C1 系统中的所有文档都具有相同的机密性。C2 系统比 C1 系统加强了可调的审慎控制。在连接到网络上时，C2 系统的用户分别对各自的行为负责。C2 系统通过登录过程、安全事件和资源隔离来增强这种控制。C2 系统具有 C1 系统中所有的安全性特征。

B 类安全等级：B 类安全等级可分为 B1、B2 和 B3 三类。B 类系统具有强制性保护功能。强制性保护意味着如果用户没有与安全等级相连，系统就不会让用户存取对象。B1 系统满足下列要求：系统对网络控制下的每个对象都进行灵敏度标记，系统使用灵敏度标记作为所有强迫访问控制的基础。系统在把导入的、非标记的对象放入系统前标记它们。灵敏度标记必须准确地表示其所联系的对象的安全级别。当系统管理员创建系统或者增加新的通信通道或 I/O 设备时，管理员必须指定每个通信通道和 I/O 设备是单级还是多级，并且管理员只能手工改变指定。单级设备并不保持传输信息的灵敏度级别，所有直接面向用户位置的输出（无论是虚拟的还是物理的）都必须产生标记来指示关于输出对象的灵敏度，系统必须使用用户的口令或证明来决定用户的安全访问级别，系统必须通过审计来记录未授权访问的企图。

B2 系统必须满足 B1 系统的所有要求。另外，B2 系统的管理员必须使用一个明确的、文档化的安全策略模式作为系统的可信任运算基础体制。B2 系统必须满足下列要求：系统必须立即通知系统中的每一个用户所有与之相关的网络连接的改变。只有用户能够在可信任通信路径中进行初始化通信，可信任运算基础体制能够支持独立的操作者和管理员。

B3 系统必须符合 B2 系统的所有安全需求。B3 系统具有很强的监视委托管理访问能力和抗干扰能力。B3 系统必须设有安全管理员。B3 系统应满足以下要求：除了控制对个别对象的访问外，B3 必须产生一个可读的安全列表，每个被命名的对象提供对该对象没有访问权的用户列表说明，B3 系统在进行任何操作前，要求用户进行身份验证。B3 系统验证每个用户，同时还会发送一个取消访问的审计跟踪消息。设计者必须正确区分可信任的通信路径和其他路径，可信任的通信基础体制为每一个被命名的对象建立安全审计跟踪，可信

任的运算基础体制支持独立的安全管理。

A 类安全等级：A 系统的安全级别最高。目前，A 类安全等级只包含 A1 一个安全类别。A1 类与 B3 类相似，对系统的结构和策略不作特别要求。A1 系统的显著特征是，系统的设计者必须按照一个正式的设计规范来分析系统。对系统分析后，设计者必须运用核对技术来确保系统符合设计规范。A1 系统必须满足下列要求：系统管理员必须从开发者那里接收到一个安全策略的正式模型，所有的安装操作都必须由系统管理员进行，系统管理员进行的每一步安装操作都必须有正式文档。

3.1.2 欧洲的安全评价标准

欧洲的安全评价标准——ITSEC 是欧洲多国安全评价方法的综合产物，应用领域为军队、政府和商业。该标准将安全概念分为功能与评估两部分。功能准则从 F1～F10 共分 10 级。1～5 级对应于 TCSEC 的 D～A。F6～F10 级分别对应数据和程序的完整性、系统的可用性、数据通信的完整性、数据通信的保密性以及机密性和完整性的网络安全。评估准则分为 6 级，分别是测试、配置控制和可控的分配、能访问详细设计和源码、详细的脆弱性分析、设计与源码明显对应以及设计与源码在形式上一致。

3.1.3 加拿大的评价标准

加拿大的评价标准——CTCPEC 专门针对政府需求而设计。与 ITSEC 类似，该标准将安全分为功能性需求和保证性需要两部分。功能性需求共划分为四大类：机密性、完整性、可用性和可控性。每种安全需求又可以分成很多小类，来表示安全性上的差别，分级条数为 0～5 级。

3.1.4 美国联邦准则

美国联邦准则——FC 是对 TCSEC 的升级，并引入了“保护轮廓”(PP)的概念。每个轮廓都包括功能、开发保证和评价三部分。FC 充分吸取了 ITSEC 和 CTCPEC 的优点，在美国的政府、民间和商业领域得到广泛应用。但 FC 有很多缺陷，是一个过渡标准，后来结合 ITSEC 发展为国际通用准则。

3.1.5 国际通用准则

国际通用准则——CC 是国际标准化组织统一现有多种准则的结果，是目前最全面的评价准则。1996 年 6 月，CC 第一版发布；1998 年 5 月，CC 第二版发布；1999 年 10 月 CC v2.1 版发布，并且成为 ISO 标准。CC 的主要思想和框架都取自 ITSEC 和 FC，并充分突出了“保护轮廓”的概念。CC 将评估过程划分为功能和保证两部分，评估等级分为 eal1、eal2、eal3、eal4、eal5、eal6 和 eal7 共 7 个等级。每一级均需评估 7 个功能类，分别是配置管理、分发和操作、开发过程、指导文献、生命期的技术支持、测试和脆弱性评估。

3.2 我国安全标准简介

我国信息安全研究经历了通信保密、计算机数据保护两个发展阶段，正在进入网络信息安全的研究阶段。通过学习、吸收、消化 TCSEC 的原则进行了安全操作系统、多级安全数

据库的研制,但由于系统安全内核受控于人,以及国外产品的不断更新升级,基于具体产品的增强安全功能的成果,难以保证没有漏洞,难以得到推广应用。在学习借鉴国外技术的基础上,国内一些部门也开发研制了一些防火墙、安全路由器、安全网关、黑客入侵检测、系统脆弱性扫描软件等。但是,这些产品安全技术的完善性、规范化实用性还存在许多不足,特别是在多平台的兼容性及安全工具的协作配合和互动性方面存在很大距离,理论基础和自主的技术手段也需要发展和强化。

以前,国内主要是等同采用国际标准。现在,由公安部主持制定、国家技术标准局发布的中华人民共和国国家标准 GB17895—1999《计算机信息系统安全保护等级划分准则》已经正式颁布并使用了。该准则将信息系统安全分为五个等级,分别是用户自主保护级、系统审计保护级、安全标记保护级、结构化保护级和访问验证保护级。主要的安全考核指标有身份认证、自主访问控制、数据完整性、审计、隐蔽信道分析、客体重用、强制访问控制、安全标记、可信路径和可信恢复等,这些指标涵盖了不同级别的安全要求。

3.2.1 第一级 用户自主保护级

本级的可信计算基通过隔离用户与数据,使用户具备自主安全保护的能力。它具有多种形式的控制能力,对用户实施访问控制,即为用户提供可行的手段,保护用户和用户组信息,避免其他用户对数据的非法读写与破坏。具体表现在如下几个方面:

(1) 可信计算基定义和控制系统中命名用户对命名客体的访问。实施机制(例如,访问控制表)允许命名用户以用户和(或)用户组的身份规定并控制客体的共享,阻止非授权用户读取敏感信息。

(2) 可信计算基初始执行时,首先要求用户标识自己的身份,并使用保护机制(例如,口令)来鉴别用户的身份,阻止非授权用户访问用户身份鉴别数据。

(3) 可信计算基通过自主完整性策略,阻止非授权用户修改或破坏敏感信息。

3.2.2 第二级 系统审计保护级

与用户自主保护级相比,本级的可信计算基实施了粒度更细的自主访问控制,它通过登录规程、审计安全性相关事件和隔离资源,使用户对自己的行为负责。它增加了客体重用以及安全审计方面的内容,并进一步增强了自主访问控制以及身份鉴别机制,具体表现在:

(1) 自主访问控制机制根据用户指定方式或默认方式,阻止非授权用户访问客体。访问控制的粒度是单个用户。控制访问权限扩散,没有存取权的用户只允许由授权用户指定对客体的访问权。

(2) 通过为用户提供唯一标识、可信计算基能够使用户对自己的行为负责。可信计算基还具备将身份标识与该用户所有可审计行为相关联的能力。

(3) 在可信计算基的空闲存储客体空间中,对客体初始指定、分配或再分配一个主体之前,撤销该客体所含信息的所有授权。当主体获得对一个已被释放的客体的访问权时,当前主体不能获得原主体活动所产生的任何信息。

(4) 可信计算基能创建和维护受保护客体的访问审计跟踪记录,并能阻止非授权的用户对它访问或破坏。可信计算基能记录下述事件:使用身份鉴别机制;将客体引入用户地址空间(例如,打开文件、程序初始化);删除客体;由操作员、系统管理员或(和)系统安全

管理员实施的动作，以及其他与系统安全有关的事件。对于每一事件，其审计记录包括事件的日期和时间、用户、事件类型、事件是否成功。对于身份鉴别事件，审计记录包含的来源（例如，终端标识符）；对于客体引入用户地址空间的事件及客体删除事件，审计记录包含客体名。对不能由可信计算基独立分辨的审计事件，审计机制提供审计记录接口，可由授权主体调用。这些审计记录区别于可信计算基独立分辨的审计记录。

3.2.3 第三级 安全标记保护级

本级的可信计算基具有系统审计保护级的所有功能。此外，还提供有关安全策略模型、数据标记以及主体对客体强制访问控制的非形式化描述；具有准确地标记输出信息的能力；消除通过测试发现的任何错误。它增加了强制访问控制机制，具体表现为：

（1）可信计算基对所有主体及其所控制的客体（例如，进程、文件、段、设备）实施强制访问控制。为这些主体及客体指定敏感标记，这些标记是等级分类和非等级类别的组合，它们是实施强制访问控制的依据。可信计算基支持两种或两种以上成分组成的安全级。可信计算基控制的所有主体对客体的访问应满足：仅当主体安全级中的等级分类高于或等于客体安全级中的等级分类，且主体安全级中的非等级类别包含了客体安全级中的全部非等级类别，主体才能读客体；仅当主体安全级中的等级分类低于或等于客体安全级中的等级分类，且主体安全级中的非等级类别包含了客体安全级中的非等级类别，主体才能写一个客体。可信计算基使用身份和鉴别数据，鉴别用户的身份，并保证用户创建的可信计算基外部主体的安全级和授权受该用户的安全级和授权的控制。

（2）可信计算基应维护与主体及其控制的存储客体（例如，进程、文件、段、设备）相关的敏感标记。这些标记是实施强制访问的基础。为了输入未加安全标记的数据，可信计算基向授权用户要求并接受这些数据的安全级别，且可由可信计算基审计。

（3）在审计记录的内容中，对于客体引入用户地址空间的事件及客体删除事件，审计记录包含客体名及客体的安全级别。此外，可信计算基具有审计更改可读输出记号的能力。

（4）在网络环境中，使用完整性敏感标记来确信信息在传送中未受损。

3.2.4 第四级 结构化保护级

本级的可信计算基建立于一个明确定义的形式化安全策略模型之上，它要求将第三级系统中的自主和强制访问控制扩展到所有主体与客体。此外，还要考虑隐蔽通道。本级的可信计算基必须结构化为关键保护元素和非关键保护元素。可信计算基的接口也必须明确定义，使其设计与实现能经受更充分的测试和更完整的复审。加强了鉴别机制；支持系统管理员和操作员的职能；提供可信设施管理；增强了配置管理控制。系统具有相当的抗渗透能力。增加的内容主要表现在如下几个方面：

（1）可信计算基对外部主体能够直接或间接访问的所有资源（例如，主体、存储客体和输入输出资源）实施强制访问控制；

（2）可信计算基能够审计利用隐蔽存储信道时可能被使用的事件；

（3）系统开发者应彻底搜索隐蔽存储信道，并根据实际测量或工程估算确定每一个被标识信道的最大带宽；

（4）对用户的初始登录和鉴别，可信计算基在它与用户之间提供可信通信路径。该路

径上的通信只能由该用户初始化。

3.2.5 第五级 访问验证保护级

本级的可信计算基满足引用监视器需求。引用监视器仲裁主体对客体的全部访问。引用监视器本身是抗篡改的；必须足够小，能够分析和测试。为了满足引用监视器需求，可信计算基在其构造时，排除那些对实施安全策略来说并非必要的代码；在设计和实现时，从系统工程角度将其复杂性降低到最小程度。支持安全管理员职能；扩充审计机制，当发生与安全相关的事件时发出信号；提供系统恢复机制。系统具有很高的抗渗透能力。增加的内容主要表现在如下几个方面：

(1) 在审计方面，可信计算基包含能够监控可审计安全事件发生与积累的机制，当超过阈值时，能够立即向安全管理员发出报警。并且，如果这些与安全相关的事件继续发生或积累，系统应以最小的代价中止它们；

(2) 可信路径上的通信只能由该用户或可信计算基激活，且在逻辑上与其他路径上的通信相隔离，且能正确地加以区分；

(3) 可信计算基提供过程和机制，保证计算机信息系统失效或中断后，可以进行不损害任何安全保护性能的恢复。

3.3 安全操作系统的基本特征

3.3.1 最小特权原则

最小特权原则是系统安全中最基本的原则之一。所谓最小特权指的是“在完成某种操作时所赋予网络中每个主体(用户或进程)必不可少的特权”。最小特权原则，则是指“应限定网络中每个主体所必需的最小特权，确保可能的事故、错误、网络部件的篡改等原因造成的损失最小”。

最小特权原则一方面给予主体“必不可少”的特权，这就保证了所有的主体都能在所赋予的特权之下完成所需要完成的任务或操作；另一方面，它只给予主体“必不可少”的特权，这就限制了每个主体所能进行的操作。

最小特权原则要求每个用户和程序在操作时应当使用尽可能少的特权，但允许主体以参与某特定工作所需要的最小特权去进入系统。被授权拥有强力角色的主体，不需要动辄运用到其所有的特权，只有在那些特权有实际需求时，主体才去运用它们。如此一来，将减少由于不注意的错误或是侵入者假装合法主体所造成的损坏发生，限制了事故、错误或攻击带来的危害。它还减少了特权程序之间潜在的相互作用，从而使对特权无意的、没必要的或不适当的使用不太可能发生。这种想法还可以引申到程序内部：只有程序中需要那些特权的最小部分才拥有特权。

3.3.2 自主访问控制和强制访问控制

自主访问控制(DAC)是一个接入控制服务，它执行基于系统实体身份和它们到系统资源的接入授权。这包括在文件、文件夹和共享资源中设置许可。

强制访问控制(MAC)是“强加”给访问主体的,即系统强制主体服从访问控制政策。强制访问控制的主要特征是对所有主体及其所控制的客体(例如,进程、文件、段、设备)实施强制访问控制。为这些主体及客体指定敏感标记,这些标记是等级分类和非等级类别的组合,它们是实施强制访问控制的依据。系统通过比较主体和客体的敏感标记来决定一个主体是否能够访问某个客体。用户的程序不能改变他自己及任何其他客体的敏感标记,从而系统可以防止特洛伊木马的攻击。

强制访问控制一般与自主访问控制结合使用,并且实施一些附加的、更强的访问限制。一个主体只有通过了自主与强制性访问限制检查后,才能访问某个客体。用户可以利用自主访问控制来防范其他用户对自己客体的攻击,由于用户不能直接改变强制访问控制属性,所以强制访问控制提供了一个不可逾越的、更强的安全保护层以防止其他用户偶然或故意地滥用自主访问控制。

强制访问策略将每个用户及文件赋予一个访问级别,如最高秘密级 T(Top Secret)、秘密级 S(Secret)、机密级 C(Confidential)及无级别级 U(Unclassified)。其级别为 T＞S＞C＞U,系统根据主体和客体的敏感标记来决定访问模式。访问模式包括:

- 下读(read down)　用户级别大于文件级别的读操作。
- 上写(write up)　用户级别小于文件级别的写操作。
- 下写(write down)　用户级别等于文件级别的写操作。
- 上读(read up)　用户级别小于文件级别的读操作。

3.3.3 安全审计功能

安全审计是识别与防止网络攻击行为、追查网络泄密行为的重要措施之一。具体包括两方面的内容:一是采用网络监控与入侵防范系统,识别网络各种违规操作与攻击行为,即时响应(如报警)并进行阻断;二是对信息内容的审计,可以防止内部机密或敏感信息的非法泄露。

审计作为安全系统的重要组成部分,在美国的 TCSEC 中对于安全审计的定义是这样的:一个安全系统中的安全审计系统,是对系统中任一或所有安全相关事件进行记录、分析和再现的处理系统。因此,在 TCSEC 中规定了对于安全审计系统的一般要求,主要包括如下的五个方面:

(1) 记录与再现,要求安全审计系统必须能够记录系统中所有的安全相关事件,同时,如果有必要,应该能够再现产生系统某一状态的主要行为;

(2) 入侵检测,安全审计系统应该能够检查出大多数常见的系统入侵的行为,同时,经过适当的设计,应该能够阻止这些入侵行为;

(3) 记录入侵行为,安全审计系统应该记录所有的入侵行为,即使某次入侵已经成功,这也是事后调查取证和系统恢复必需的;

(4) 威慑作用,应该对系统中具有的安全审计系统及其性能进行适当宣传,这样可以对企图入侵者起到威慑作用,又可以减少合法用户在无意中违反系统的安全策略;

(5) 系统本身的安全性,安全审计系统本身的安全性必须保证,这包括两个方面的内容,一是操作系统和软件的安全性,另一个是审计数据的安全性;一般来说,要保证审计系统本身的安全,必须与系统中其他安全措施(例如认证、授权、加密等)相配合。

另外,TCSEC 还要求 C2 级以上的安全操作系统必须包含审计功能。我国计算机信息系统安全保护等级划分准则(GB 17859—1999)对安全审计也有相应的要求。审计为系统进行事故原因的查询、定位、事故发生前的预测、报警以及事故发生之后的实时处理提供详细、可靠的依据和支持,以便有违反系统安全规则的事件发生后能够有效地追查事件发生的地点和过程。

3.3.4 安全域隔离功能

安全域是指在其中实施认证、授权和访问控制的安全策略的计算环境。当用户安装和配置操作系统时,将创建称为管理域的初始安全域。安全域理论不仅为建设信息安全保障体系提供基础,而且在风险评估当中如果能较好地应用安全域,还会起到事半功倍的作用。安全域可以将一个单独资产联系起来,在等级保护当中也有比较好的应用。总之,安全域理论是安全方面的最佳实践,对于信息安全建设具有非常重要的指导意义。

3.4 Windows 2003 的安全设置

3.4.1 Windows 安全漏洞及其解决建议

Windows 系统上的重大安全漏洞,主要包括两大部分:Windows 服务器安全漏洞和工作站的安全漏洞。

对于这些安全漏洞更佳的解决方案是建设一个强壮的防火墙,精心地配置它,只授权给可信赖的主机能通过防火墙。在防火墙上,截止所有从端口 137～139 的 TCP 和 UDP 连接,这样做有助于对远程连接的控制。另外,在内部路由器上,设置 ACL,在各个独立子网之间,截止从端口 137～139 的连接。这是一种辅助措施,以限制该安全漏洞。值得注意的是,有些黑客程序可以具有选择端口号的能力,它可能成功地攻击其他端口。

3.4.2 Windows 2003 的认证机制

Windows 2003 身份认证的重要功能就是它对单一注册的支持。单一注册允许用户使用一个密码一次登录到域,然后向域中的任何计算机认证身份。

单一注册在安全性方面提供了两个主要优点:对用户而言,单个密码或智能卡的使用减少了混乱,提高了工作效率;对管理员而言,由于管理员只需要为每个用户管理一个账户,域用户所要求的管理支持减少了。

身份认证分以下两种方式执行:

(1) 交互式登录。交互式登录过程向域账户或本地计算机确认用户的身份,这一过程根据用户账户的类型而不同。如果使用域账户登录,被授权的用户可以访问该域以及任何信任域中的资源。如果使用密码登录到域账户,Windows 2003 将使用 Kerberos V5 进行身份认证。如果使用智能卡,Windows 2003 将使用带证书的 Kerberos V5 身份认证。

(2) 网络身份认证。网络身份认证确认用户对于试图访问的任意网络服务的身份。为了提供这种类型的身份认证,Windows 2003 安全系统支持多种不同的身份认证机制,包括 Kerberos V5、安全套接字层/传输层安全(SSL/TLS)以及为了与 Windows NT 4.0 兼容而

提供的 NTLM。

3.4.3 Windows 2003 账号安全

（1）域用户账号。域用户账号是用户访问域的唯一凭证，因此在域中必须是唯一的。域用户账号在域控制器上建立，作为活动目录的一个对象保存在域的数据库中。用户在从域中的任何一台计算机登录到域中的时候必须提供一个合法的域用户账号，该账号将被域控制器所验证。

（2）本地用户账号。本地用户账号只能建立在 Windows 2003 独立服务器上，以控制用户对该计算机资源的访问。

（3）内置的用户账号。Administrator（管理员）账号被赋予在域中和在计算机中具有不受限制的权利，该账号被设计用于对本地计算机或域进行管理，可以从事创建其他用户账号、创建组、实施安全策略、管理打印机以及分配用户对资源的访问权限等工作。Guest（来宾）账号一般被用于在域中或计算机中没有固定账号的用户临时访问域或计算机时使用的。该账号默认情况下不允许对域或计算机中的设置和资源做永久性的更改。出于安全考虑，Guest 账号在 Windows 2003 安装好之后是被屏蔽的。如果需要，可以手动启动，应该注意分配给该账号的权限，该账号也是黑客攻击的主要对象。

（4）账号命名约定。由于账号在域中的重要性和唯一性，因此账号的命名约定十分重要。一个好的账号命名约定将有助于规划一个高效的活动目录。Windows 2003 的账号命名约定包括如下内容：

① 域用户账号的用户登录名在活动目录中必须唯一。

② 域用户账号的完全名称在创建该用户账号的域中必须唯一。

③ 本地用户账号在创建该账号的计算机上必须唯一。

④ 如果用户名称有重复，则应该在账号上区别出来。

（5）密码约定。通常设定密码有如下原则：

① 尽量避免带有明显意义的字符或数字的组合，最好采用大小写和数字的无意义混合。在不同安全要求下，规定最小的密码长度。通常密码越长越不易被猜到（最长可以达到 128 位）。

② 对于不同级别的安全要求，确定用户的账号密码是由管理员控制还是由账号的拥有者控制。

③ 定期更改密码，尽量使用不同的密码。有关密码的策略可以由系统管理员在密码策略管理工具中加以规定，以保护系统的安全性。

3.4.4 Windows 2003 文件系统安全

文件系统安全是操作系统安全的核心。Windows 2003 文件系统控制谁能访问信息以及他们能做些什么。即使外层账号安全被突破，攻击者还必须击败文件系统根据文件拥有权和权限精心设置的防御措施。当建立文件的权限时，必须先确定文件系统格式为 Windows NT 文件系统（NTFS），当然也可以使用 FAT 格式，但是并不支持文件级的权限。一旦已经实施了 NTFS 的文件系统格式，就可通过 Windows 的资源管理器直接来管理文件的安全。

NTFS 权限及使用有以下几个原则：

（1）权限最大原则。当一个用户同时属于多个组，而这些组又有可能被赋予了对某种资源的不同访问权限，则用户对该资源最终有效权限是在这些组中最宽松的权限，即加权权限，将所有的权限加在一起即为该用户的权限（"完全控制"权限为所有权限的总和）。

（2）文件权限超越文件夹权限原则。当用户或组对某个文件夹以及该文件夹下的文件有不同的访问权限时，用户对文件的最终权限是访问该文件的权限，即文件权限超越文件的上级文件夹的权限，用户访问该文件夹下的文件不受文件夹权限的限制，而只受被赋予的文件权限的限制。

（3）拒绝权限超越其他权限原则。当用户对某个资源有拒绝权限时，该权限覆盖其他任何权限，即在访问该资源的时候只有拒绝权限是有效的。当有拒绝权限时权限最大法则无效。因此对于拒绝权限的授予应该慎重考虑。

在同一个 NTFS 分区内或不同的 NTFS 分区之间移动或复制一个文件或文件夹时，该文件或文件夹的 NTFS 权限会发生不同的变化。这时 NTFS 权限的继承性就起到了作用，关于 NTFS 权限的继承性有以下几个方面：

（1）在同一个 NTFS 分区内移动文件或文件夹。在同一分区内移动的实质就是在目的位置将原位置上的文件或文件夹"搬"过来，因此文件和文件夹仍然保留有在原位置的一切 NTFS 权限（准确地讲就是该文件或文件夹的权限不变）。

（2）在不同 NTFS 分区之间移动文件或文件夹。在这种情况下文件和文件夹会继承目的分区中文件夹的权限（ACL），实质就是在原位置删除该文件或文件夹，并且在目的位置新建该文件或文件夹（要从 NTFS 分区中移动文件或文件夹，操作者必须具有相应的权限。在原位置上必须有"修改"的权限，在目的位置上必须有"写"权限）。

（3）在同一个 NTFS 分区内复制文件或文件夹，在这种情况下复制文件和文件夹将继承目的位置中的文件夹的权限。

（4）在不同 NTFS 分区之间复制文件或文件夹，在这种情况下复制文件和文件夹将继承目的位置中文件夹的权限（当从 NTFS 分区向 FAT 分区中复制或移动文件和文件夹都将导致文件和文件夹的权限丢失，因为 FAT 分区不支持 NTFS 权限）。

3.4.5 Windows 文件保护

微软公司为 Windows 2000/XP 系统增添了一项新功能 WFP（Windows File Protection）。这个组件的主要功能是，在系统文件遭到意外删除，或在安装/卸载应用程序时被无意识破坏后，利用备份文件恢复 Windows 系统。

初次安装 Windows XP 时，部分以 dll、exe、fon、ocx、sys 和 tff 结尾的文件将被 WFP 标识为重要的系统文件，并在 dllcache 文件夹下为这些文件备份。在用户使用 Windows 2000/XP 系统的过程中，WFP 将在默认设置下把以 ax、cpl、cpx、dll、exe、fon、inf、ocx、rsp、sys、tff 和 tlb 结尾的文件备份在 WINDOWS\system32\dllcache 文件夹下。如果这些系统文件被误删除或是被破坏，WFP 能够利用在 dllcache 下的备份文件，轻而易举地恢复 Windows 的文件系统。

由于 WFP 能自动利用备份恢复原有系统文件，所以不能用一般的方法升级装有 WFP 的操作系统文件。下面介绍几种升级的常用方法：

(1) 安装 Windows 服务组件。

(2) 升级 Windows 系统。

(3) 运行 hotfix.exe。hotfix 能自动更新 WFP 所备份的系统文件。目前大多数 hotfix 程序已经被打包在 Windows 服务组件内。如果安装了 Windows XP SP1,那么打开"添加/删除程序"能看到两个 hotfix 程序。

(4) 使用 Winnt32.exe 运行系统的安装/升级程序。

此外,还有一种简单的手工升级方法,把要升级的文件复制到 dllcache 文件夹下,然后 WFP 就能自动升级 Windows 文件系统。

在运行 WFP 程序之前,用户必须先以系统管理员身份登录。系统管理员的身份会为用户修改与 WFP 有关的配置提供相当方便的条件。在完成相关设置后,退出系统以正常用户身份再次登录,这样就可以使用 WFP 了。

3.4.6 Windows 2003 的加密机制

文件加密系统(Encryption File System,EFS)是 Windows 2003/XP 所特有的一个实用功能,对于 NTFS 卷上的文件和数据,都可以直接被操作系统加密保存,在很大程度上提高了数据的安全性。

EFS 加密是基于公钥策略的。在使用 EFS 加密一个文件或文件夹时,系统首先会生成一个由伪随机数组成的文件密钥(File Encryption Key,FEK),然后将利用 FEK 和数据扩展标准 X 算法创建加密后的文件,并把它存储到硬盘上,同时删除未加密的原始文件。随后系统利用公钥加密 FEK,并把加密后的 FEK 存储在同一个加密文件中。而在访问被加密的文件时,系统首先利用当前用户的私钥解密 FEK,然后利用 FEK 解密出文件。在首次使用 EFS 时,如果用户还没有公钥/私钥对(统称为密钥),则会首先生成密钥,然后加密数据。如果登录到了域环境中,密钥的生成依赖于域控制器,否则它就依赖于本地机器。

EFS 加密有以下两点好处,首先,EFS 加密机制和操作系统紧密结合,因此不必为了加密数据安装额外的软件,这节约了使用成本。其次,EFS 加密系统对用户是透明的。这也就是说,如果加密了一些数据,那么对这些数据的访问将是完全允许的,并不会受到任何限制。而其他非授权用户试图访问加密过的数据时,就会收到"访问拒绝"的错误提示。EFS 加密的用户验证过程是在登录 Windows 时进行的,只要登录到 Windows,就可以打开任何一个被授权的加密文件。

要使用 EFS 加密,首先要保证操作系统符合要求。目前支持 EFS 加密的 Windows 操作系统主要有 Windows 2000、Windows Server 2003 全部版本和 Windows XP Professional。其次,EFS 加密只对 NTFS 5 分区上的数据有效(注意,这里提到了 NTFS 5 分区,这是指由 Windows 2003/XP 格式化过的 NTFS 分区;而由 Windows NT 格式化的 NTFS 分区是 NTFS 4 格式的,虽然同样是 NTFS 文件系统,但它不支持 EFS 加密),无法加密保存在 FAT 和 FAT 32 分区上的数据。

对于想加密的文件或文件夹,只需要用鼠标右键单击,然后选择"属性",在常规选项卡下单击"高级"按钮,之后在弹出的窗口中选中"加密内容以保护数据",然后单击"确定"按钮,等待片刻数据就加密好了。如果加密的是一个文件夹,系统还会询问,是把这个加密属性应用到文件夹上还是文件夹以及内部的所有子文件夹。按照实际情况来操作即可。解密

数据也是很简单的，同样是按照上面的方法，把“加密内容以保护数据”前的钩消除，然后单击“确定”按钮。

注意：如果把未加密的文件复制到具有加密属性的文件夹中，这些文件将会被自动加密。若是将加密数据移出来，如果移动到 NTFS 分区上，数据依旧保持加密属性；如果移动到 FAT 分区上，这些数据将会被自动解密。被 EFS 加密过的数据不能在 Windows 中直接共享。如果通过网络传输经 EFS 加密过的数据，这些数据在网络上将会以明文的形式传输。NTFS 分区上保存的数据还可以被压缩，不过一个文件不能同时被压缩和加密。最后一点，Windows 的系统文件和系统文件夹无法被加密。

3.4.7 Windows 2003 的安全配置

安全配置是侧重于减少攻击面的安全策略设置工具。使用安全配置可以执行以下操作：

禁用不必要的端口和服务、配置 Microsoft Windows 防火墙、配置 Internet 协议安全(IPSEC)筛选器、配置轻型目录访问协议(LDAP)设置、配置服务器消息块(SMB)设置、配置 NTLM 协议设置、配置预定义的审核设置等。

常用的安全配置组件有本地安全策略、组策略、注册表编辑器、防火墙设置、计算机管理、服务等，这些组件的应用在第 12 章中将会详细讲解，下面只对本地安全策略和组策略进行简单的介绍。

1. 本地安全策略

Windows 系统自带的“本地安全策略”是一个很不错的系统安全管理工具。它可以对本机的许多属性(例如用户、密码、审核、用户权限分配等)进行设置，这些设置只影响本计算机的安全设置。

启用 Windows 2003 的管理工具“本地安全策略”，依次选择“开始”→“程序”→“管理工具”→“本地安全策略”命令，打开“本地安全设置”窗口，如图 3.2 所示，主要包括“账户策略”、“本地策略”、IP 安全策略配置等。

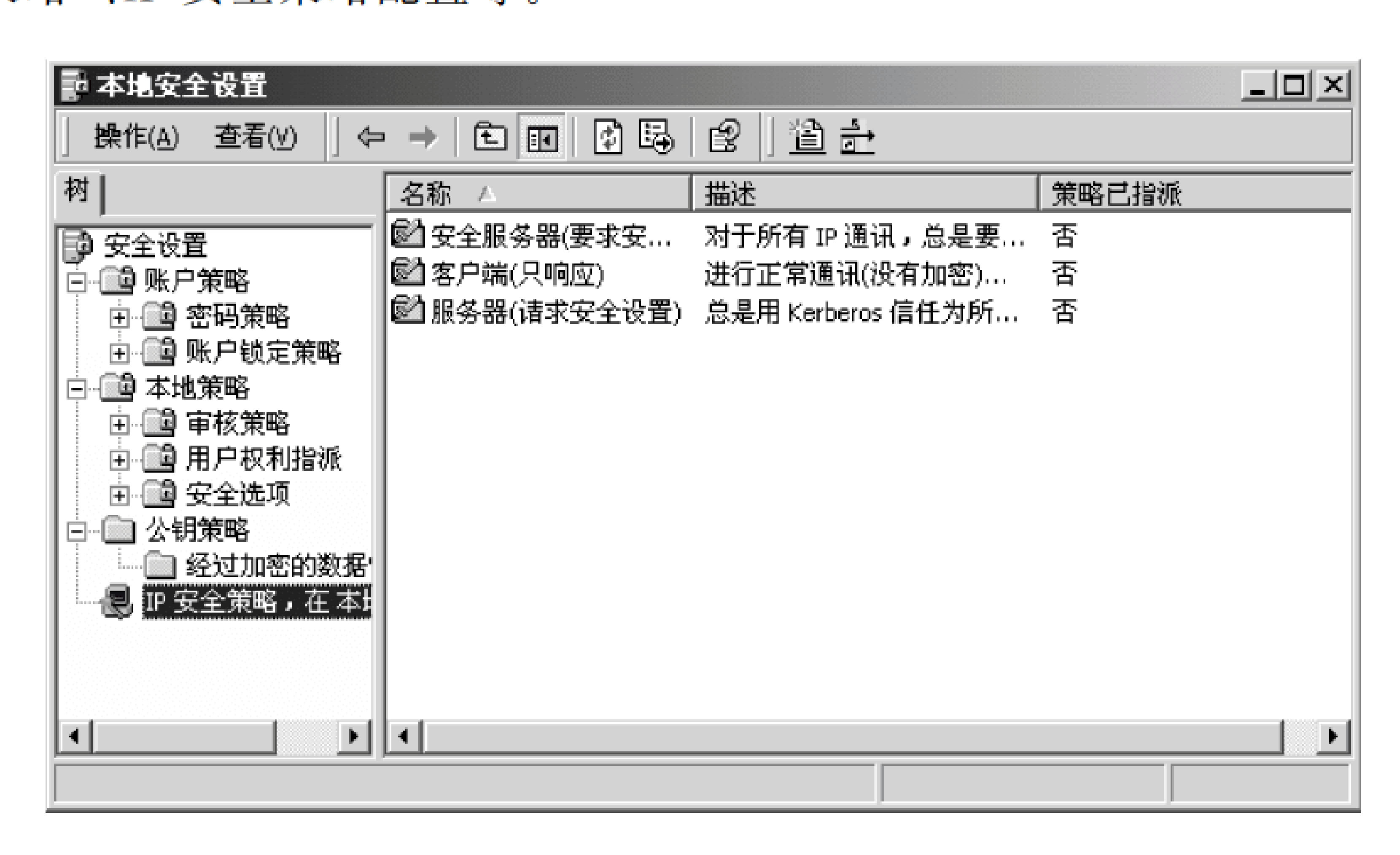


图 3.2 系统安全配置

2. 组策略

所谓组策略，顾名思义，就是基于组的策略。它以 Windows 中的一个 MMC 管理单元的形式存在，可以帮助系统管理员针对整个计算机或是特定用户来设置多种配置，包括桌面配置和安全配置。譬如，可以为特定用户或用户组定制可用的程序、桌面上的内容，以及“开始”菜单选项等，也可以在整个计算机范围内创建特殊的桌面配置。简而言之，组策略是 Windows 中的一套系统更改和配置管理工具的集合。组策略修改注册表中的配置。当然，组策略使用自己更完善的管理组织方法，可以对各种对象中的设置进行管理和配置，远比手工修改注册表方便、灵活，功能也更加强大。

组策略编辑器的启动很简单，只需选择“开始”→“运行”命令，在“运行”对话框中输入 gpedit. msc，然后单击“确定”按钮即可启动 Windows XP 组策略编辑器。

例如要启动 Windows 的文件保护功能，只需打开“组策略”窗口，在左侧列表里展开“计算机设置”→“管理模板”→“系统”→“Windows 文件保护”，在右侧列表中显示已有的文件保护策略，如图 3.3 所示，双击列表中的某项，打开设置窗口。在该窗口中可设置“已启用”这一项安全策略。这样就实现了 Windows 的文件保护功能。



图 3.3　Windows 文件保护

3.4.8　Windows 2003 文件和数据的备份

如果系统的硬件或存储媒体发生故障，“备份”工具可以帮助用户保护数据免受意外的损失。例如，可以使用“备份”创建硬盘中数据的副本，然后将数据存储到其他存储设备。备份存储媒体既可以是逻辑驱动器(如硬盘)、独立的存储设备(如可移动磁盘)，也可以是由自动转换器组织和控制的整个磁盘库或磁带库。如果硬盘上的原始数据被意外删除或

覆盖，或因为硬盘故障而不能访问该数据，那么可以十分方便地从存档副本中还原该数据。为了保护服务器，应该安排对所有数据进行定期备份。数据备份的类型大致分为以下几种：

(1) 副本备份，可以复制所有选定的文件，但不将这些文件标记为已经备份(换言之，不清除存档属性)。如果要在正常和增量备份之间备份文件，复制是很有用的，因为它不影响其他备份操作。

(2) 每日备份，用于复制执行每日备份的当天修改过的所有选定文件。备份的文件将不会标记为已经备份(换言之，不清除存档属性)。

(3) 差异备份，用于复制自上次正常或增量备份以来所创建或更改的文件。它不将文件标记为已经备份(换言之，不清除存档属性)。如果要执行正常备份和差异备份的组合，则还原文件和文件夹将需要上次已执行过正常备份和差异备份。

(4) 增量备份，仅备份自上次正常或增量备份以来创建或更改的文件。它将文件标记为已经备份(换言之，清除存档属性)。如果将正常和增量备份结合使用，需要具有上次的正常备份集和所有增量备份集才能还原数据。

(5) 正常备份，用于复制所有选定的文件，并且在备份后标记每个文件(换言之，清除存档属性)。使用正常备份，只需备份文件或磁带的最新副本就可以还原所有文件。通常，在首次创建备份集时执行一次正常备份。

组合使用正常备份和增量备份来备份数据，需要的存储空间最少，并且是最快的备份方法。然而，恢复文件可能比较耗时而且比较困难，因为备份集可能存储在不同的磁盘或磁带上。

组合使用正常备份和差异备份来备份数据更加耗时，尤其当数据经常更改时，但是它更容易还原数据，因为备份集通常只存储在少量磁盘和磁带上。

Windows 2003 自带的备份工具如图 3.4 所示，具体备份方法请参见第 12 章的内容。

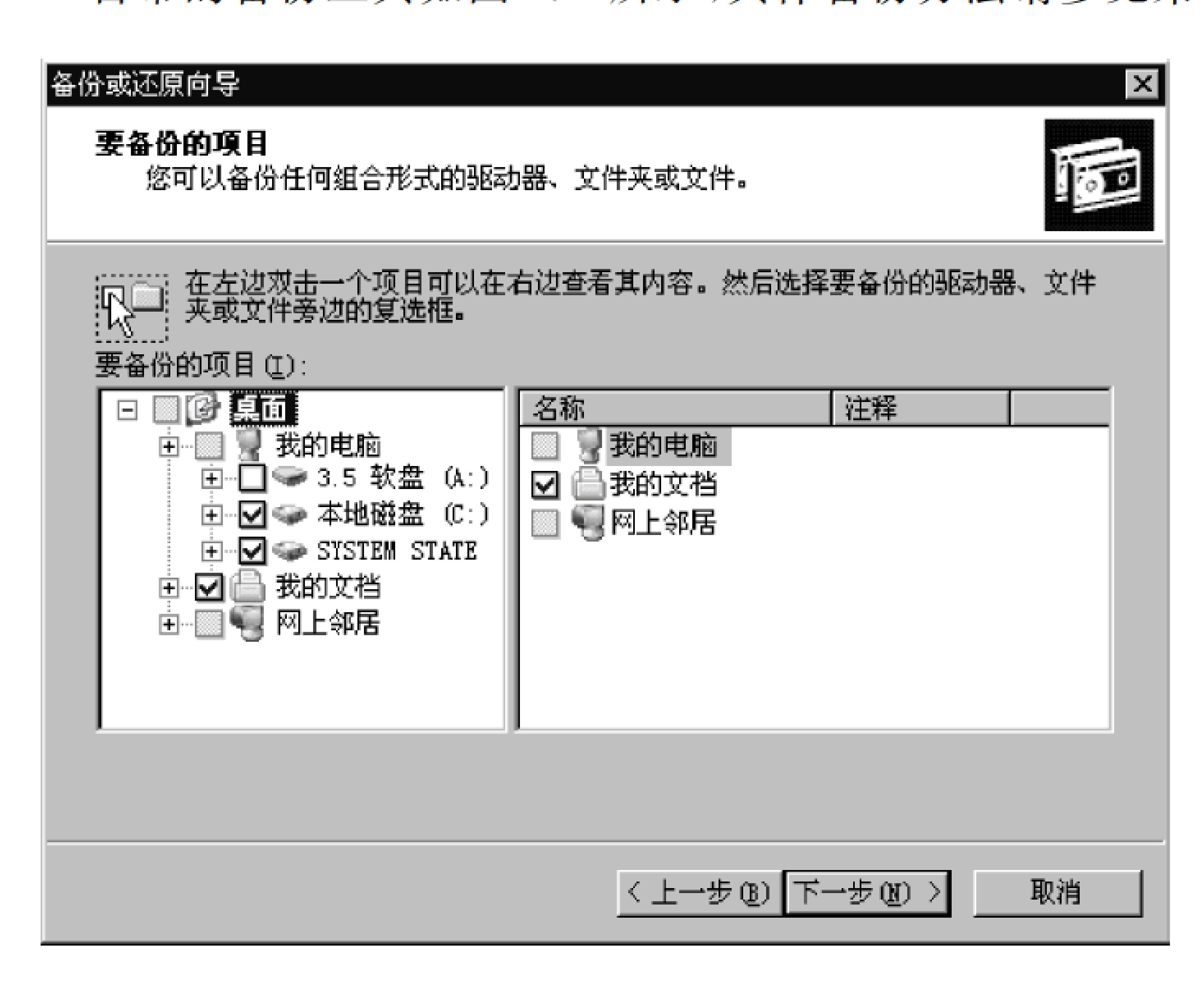


图 3.4　备份和还原工具

课 后 习 题

选择题

1. Windows 主机推荐使用(　　)格式。

A. NTFS　　B. FAT32　　C. FAT　　D. LINUX

2. 对文件和对象的审核,错误的一项是(　　)。

A. 文件和对象访问的成功和失败　　B. 用户及组管理的成功和失败

C. 安全规则更改的成功和失败　　D. 文件名更改的成功和失败

3. 不属于服务器的安全措施的是(　　)。

A. 保证注册账户的时效性

B. 删除死账户

C. 强制用户使用不易被破解的密码

D. 所有用户使用一次性密码

4. 不属于数据备份类型的是(　　)。

A. 每日备份　　B. 差异备份　　C. 增量备份　　D. 随机备份

填空题

1. 计算机系统安全评估的第一个正式标准是(　　)

2. 自主访问控制(DAC)是一个接入控制服务,它执行基于系统实体身份和它们到系统资源的接入授权。这包括在文件、(　　)和(　　)中设置许可。

3. 安全审计是识别与防止(　　)、追查(　　)的重要措施之一。

4. Windows 系统上的重大安全漏洞,主要包括两大部分:(　　)和(　　)的安全漏洞。

5. (　　)账号一般被用于在域中或计算机中没有固定账号的用户临时访问域或计算机时使用的。

6. (　　)账号被赋予在域中和在计算机中具有不受限制的权利,该账号被设计用于对本地计算机或域进行管理,可以从事创建其他用户账号、创建组、实施安全策略、管理打印机以及分配用户对资源的访问权限等工作。

7. 中华人民共和国国家标准 GB17895—1999《计算机信息系统安全保护等级划分准则》已经正式颁布并使用了。该准则将信息系统安全分为五个等级,分别是自主保护级、(　　)、(　　)、(　　)和访问验证保护级。

简答题

1. 简述 TCSEC 中的 C1、C2、B1 级的主要安全要求。

2. 简述审核策略、密码策略和账户策略的含义。这些策略如何保护操作系统不被入侵? P206 如何关闭不需要的端口和服务?

3. 计算机安全评价标准中 B 类安全等级都包括哪些内容?

4. 计算机安全评价标准中 A 类安全等级都包括哪些内容?

5. 计算机信息系统安全保护等级划分准则中将信息系统安全分为几个等级? 主要的

安全考核指标是什么？

6. 安全操作系统的基本特征有哪些？

7. Windows 2000 的账号命名约定包括哪些内容？

8. NTFS 的权限及使用原则有哪些？

9. 有利于提高系统安全性的设置有哪些？

10. 本地安全策略由哪几部分组成？

第4章 密码技术

密码学是研究如何隐秘地传递信息的学科。在现代特别指对信息以及其传输的数学性研究,常被认为是数学和计算机科学的分支,和信息论也密切相关。著名的密码学者 Ron Rivest 解释道:“密码学是关于如何在敌人存在的环境中通信”。自工程学的角度,这相当于密码学与纯数学的异同。密码学是信息安全等相关议题(如认证、访问控制等)的核心。密码学的首要目的是隐藏信息的含义,而不是隐藏信息的存在。密码学也促进了计算机科学的发展,特别是计算机与网络安全所使用的技术,如访问控制与信息的机密性。密码学已被应用在日常生活的各个方面,这包括自动柜员机的芯片卡、计算机使用者存取密码、电子商务等。

密码学的目的可以概括为以下三点:

(1) 保障信息安全的重要手段;

(2) 防止信息泄露和失密的有效措施;

(3) 提高关键信息保密水平。

4.1 密码学的起源

密码学根据其研究的范围可分为密码编码学和密码分析学。密码编码学是研究密码体制的设计,对信息进行编码实现隐蔽信息的一门学问;密码分析学是研究如何破译被加密信息或信息伪造的学问。它们是相互对立、相互依存、相互促进并发展的。密码学的发展大致可以分为三个阶段:

第一阶段是从几千年前到1949年。这一时期密码学还没有成为一门真正的科学,而是一门艺术。密码学专家常常是凭自己的直觉和信念来进行密码设计,而对密码的分析也多基于密码分析者(即破译者)的直觉和经验来进行的。

世界上最早的一种密码产生于公元前2世纪。是由一位希腊人提出的,人们称之为棋盘密码,因为该密码将26个字母放在5×5的方格里,i、j放在一个格子里,具体情况如表4.1所示。

这样,每个字母就对应了由两个数构成的字符 α、β,α 是该字母所在行的标号,β 是列标号。如c对应13,s对应43等。如果接收到密文为

43 15 13 45 42 15 32 15 43 43 11 22 15,则对应的明文即为 secure message。

另一种具有代表性的密码是凯撒密码。它是将英文字母向前推移 k 位。如 $k=5$,则密文字母与明文有如下对应关系:

a b c d e f g h i j k l m n o p q r s t u v w x y z

F G H I J K L M N O P Q R S T U V W X Y Z A B C D E

表 4.1 棋盘密码

行\列	1	2	3	4	5
1	a	b	c	d	e
2	f	g	h	i、j	k
3	l	m	n	o	p
4	q	r	s	t	u
5	v	w	x	y	z

于是对应于明文 secure message，可得密文为 XJHZWJRJXXFLJ。此时，k 就是密钥。为了传送方便，可以将 26 个字母一一对应于 0～25 的 26 个整数。如 a 对 1、b 对 2……y 对 25、z 对 0。这样凯撒加密变换实际就是一个同余式：

$$c \equiv m + k \mod 26$$

其中，m 是明文字母对应的数，c 是与明文对应的密文的数。

随后，为了提高凯撒密码的安全性，人们对凯撒密码进行了改进。选取 k、b 作为两个参数，其中要求 k 与 26 互素，明文与密文的对应规则为：

$$c \equiv km + b \mod 26$$

可以看出，$k=1$ 就是前面提到的凯撒密码。于是这种加密变换是凯撒加密变换的推广，并且其保密程度也比凯撒密码高。

以上介绍的密码体制都属于单表置换。意思是一个明文字母对应的密文字母是确定的。根据这个特点，利用频率分析可以对这样的密码体制进行有效的攻击。方法是在大量的书籍、报刊和文章中，统计各个字母出现的频率。例如，e 出现的次数最多，其次是 t、a、o、l 等。破译者通过对密文中各字母出现频率的分析，结合自然语言的字母频率特征，就可以将该密码体制破译。

鉴于单表置换密码体制具有这样的攻击弱点，人们自然就会想办法对其进行改进，来弥补这个弱点，增加抗攻击能力。法国密码学家维吉尼亚于 1586 年提出一个种多表式密码，即一个明文字母可以表示成多个密文字母。其原理是这样的：给出密钥 $K=k[1]k[2]\cdots k[n]$，若明文为 $M=m[1]m[2]\cdots m[n]$，则对应的密文为 $C=c[1]c[2]\cdots c[n]$。其中 $C[i]=(m[i]+k[i]) \mod 26$。例如，若明文 M 为 data security，密钥 k=best，将明文分解为长为 4 的序列 data secu rity，对每 4 个字母，用 k=best 加密后得密文为 C=EELT TIUN SMLR，从中可以看出，当 K 为一个字母时，就是凯撒密码。而且容易看出，K 越长，保密程度就越高。显然这样的密码体制比单表置换密码体制具有更强的抗攻击能力，而且其加密、解密均可用所谓的维吉尼亚方阵来进行，从而在操作上简单易行。该密码曾被认为是三百年内破译不了的密码，因而这种密码在今天仍被使用着。

隐写术是最为人们所熟悉的古典加密方法，它通常将秘密消息隐藏于其他消息中，使真正的秘密通过一份无伤大雅的消息发送出去。隐写术分为两种，技术隐写术和语言隐写术。技术方面的隐写比较容易想象：比如不可见的墨水，洋葱法和牛奶法也被证明是普遍且有效的方法（只要在背面加热或紫外线照射即可复现）。语言隐写术与密码编码学关系比较密切，它主要提供两种类型的方法：符号码和公开代码。

符号码是以可见的方式，如手写体字或图形，隐藏秘密的书写。在书或报纸上标记所选择的字母，比如用点或短划线，这比上述方法更容易被人怀疑，除非使用显隐墨水，但此方法易于实现。一种变形的应用是降低所关心的字母，使其水平位置略低于其他字母，但这种降低几乎让人觉察不到。

一份秘密的信件或伪装的消息要通过公开信道传送，需要双方事前的约定，也就是需要一种公开代码。这可能是保密技术的最古老形式，公开文献中经常可以看到。东方和远东的商人和赌徒在这方面有独到之处，他们非常熟练地掌握了手势和表情的应用。在美国的纸牌骗子中较为盛行的方法有：手拿一支烟或用手挠一下头，表示所持的牌不错；一只手放在胸前并且跷起大拇指，意思是"我将赢得这局，有人愿意跟我吗?"右手手掌朝下放在桌子上，表示"是"，手握成拳头表示"不"。

特定行业或社会阶层经常使用的语言，往往被称为行话。一些乞丐、流浪汉及地痞流氓使用的语言还被称为黑话，它们是这些社会群体的护身符。其实也是利用了伪装，伪装的秘密因此也称为专门隐语。

黑社会犯罪团伙使用的语言特别具有隐语的特性，法语中黑话有很多例子，其中有的现在还成了通俗用法。比如 rossignol（夜莺）表示"万能钥匙"，最早始于 1460 年；mouche（飞行）表示"告密者"等。

公开代码的第二种类型就是利用虚码和漏格进行隐藏，隐藏消息的规则比较常见的有："某个特定字符后的第几个字符"，比如空格后的下一个字母（"家庭代码"，"二战"中在参战士兵中广为流传，但引起了审查机关的极大不满）；更好一点的还有空格后的第三个字母，或者标点符号后的第三个字母。

漏格方法可以追溯到卡达诺（Cardano，1550 年）时代，这是一种容易掌握的方法，但不足之处是双方需要相同的漏格，特别是战场上的士兵，使用时不太方便。

在第二次世界大战中，德军曾一度使用一种被称为 BCHI 的双重纵行换位密码，而且作为陆军和海军的应急密码，只不过密钥字每天变换，并且在陆军团以下单位使用。此时英国人早就能解读消息了，两个不同的密钥字甚至三重纵行换位的使用也无济于事。

随着电动打字机的使用，电动密码机开始在保密通信中大显身手。在第二次世界大战中，转轮密码机的使用相当普遍。它主要利用机械运动和简单电子线路，有一个键盘和若干转轮，实际上它是维吉尼亚密码的一种实现。每个转轮由绝缘的圆形胶板组成，胶板正反两面边缘线上有金属凸块，每个金属凸块上标有字母，字母的位置相互对齐。胶板正反两面的字母用金属连线接通，形成一个置换运算。不同的转轮固定在一个同心轴上，它们可以独立自由转动，每个转轮可选取一定的转动速度。例如，一个转轮可能被导线连通以完成用 F 代替 A、用 U 代替 B、用 L 代替 C 等。

为了防止密码分析，有的转轮密码机还在每个转轮上设定不同的位置号，使得转轮的位置、转轮的数量、转轮上的齿轮结合起来，增大机器的周期。

最著名的转轮密码机是德国人舍尔比乌斯设计的恩尼格马机和瑞典人哈格林设计的哈格林密码机（美国军方称为 M-209）。

德国人使用的恩尼格马机共有五个转轮，可选择三个使用。如图 4.1 所示，转轮机中设计的一块插板及一个反射轮，可对一个明文字母操作两次。另一个特点是转轮由齿轮控制，以形成不规则进位。波兰的密码研究人员最早破译了德国的恩尼格马机，并将方法提供给

了英国人。

M-209 是“二战”中美军的主要加密设备，它是一种齿数可变的齿轮装置，有六个密钥轮，一个印字轮。在一次特定的加密作业中，有多少个齿，代替表就推移多少个位置，并用这个代替表加密。该设备的各个部件互相作用，产生一串互不相关的长周期密钥。

太平洋战争中，美军破译了日本海军的密码机，读懂了日本舰队司令官山本五十六发给各指挥官的命令，在中途岛彻底击溃了日本海军，导致了太平洋战争的决定性转折，而且不久还击毙了山本五十六。相反轴心国中，只有德国在第二次世界大战的初期取得过密码破译的辉煌战绩。因此，可以说，密码学在战争中起着非常重要的作用。

古典密码的发展已有悠久的历史了，尽管这些密码大都比较简单，但它在今天仍有广泛的使用。





图 4.1　恩尼格马转轮密码机

第二阶段是从 1949 年到 1975 年。1949 年，美国数学家、信息论的创始人克劳德·香农发表了《保密系统的信息理论》一文，它标志着密码学阶段的开始。同时以这篇文章为标志的信息论为对称密钥密码系统建立了理论基础，从此密码学成为一门科学。由于保密的需要，这时人们基本上看不到关于密码学的文献和资料，平常人们是接触不到密码的。1967 年 David Kahn 出版了一本叫做《破译者》的小说，使人们知道了密码学。20 世纪 70 年代初期，IBM 发表了有关密码学的几篇技术报告，从而使更多的人了解了密码学的存在。但科学理论的产生并没有使密码学失去艺术的一面，如今，密码学仍是一门具有艺术性的科学。

第三阶段为 1976 年至今。1976 年，Diffie 和 Hellman 发表了《密码学的新方向》一文，他们首次证明了在发送端和接收端不需要传输密钥的保密通信的可能性，从而开创了公钥密码学的新纪元。该文章也成了区分古典密码和现代密码的标志。1977 年，美国的数据加密标准(DES)公布。这两件事情导致了对密码学的空前研究。从这时候起，开始对密码在民用方面进行研究，密码才开始充分发挥它的商用价值和社会价值，人们才开始能够接触到密码学。这种转变也促使了密码学的空前发展。

密码是通信双方按约定的法则进行信息特殊变换的一种重要保密手段。依照这些法则，变明文为密文，称为加密变换；变密文为明文，称为解密变换。密码在早期仅对文字或数码进行加、解密变换，随着通信技术的发展，对语音、图像、数据等都可实施加、解密变换。

密码学是在编码与破译的斗争实践中逐步发展起来的，并随着先进科学技术的应用，已成为一门综合性的尖端技术科学。它与语言学、数学、电子学、声学、信息论、计算机科学等有着广泛而密切的联系。它的现实研究成果，特别是各国政府现用的密码编制及破译手段都具有高度的机密性。

4.2　密码学中的重要术语

- 明文(plaintext)：需要被隐蔽的消息。
- 密文(ciphertext)：明文经变换形成的隐蔽形式。
- 加密(encryption)：从明文到密文的变换过程。
- 解密(decryption)：从密文恢复到明文的过程。

变换函数所用的一个控制参数称为密钥(key)。

加密和解密算法的操作通常是在一组密钥控制下进行的，分别称为加密密钥和解密密钥。密钥未知情况下进行的解密推演过程，称为破译，也称为密码分析或者密码攻击。它们之间的关系如图 4.2 所示。

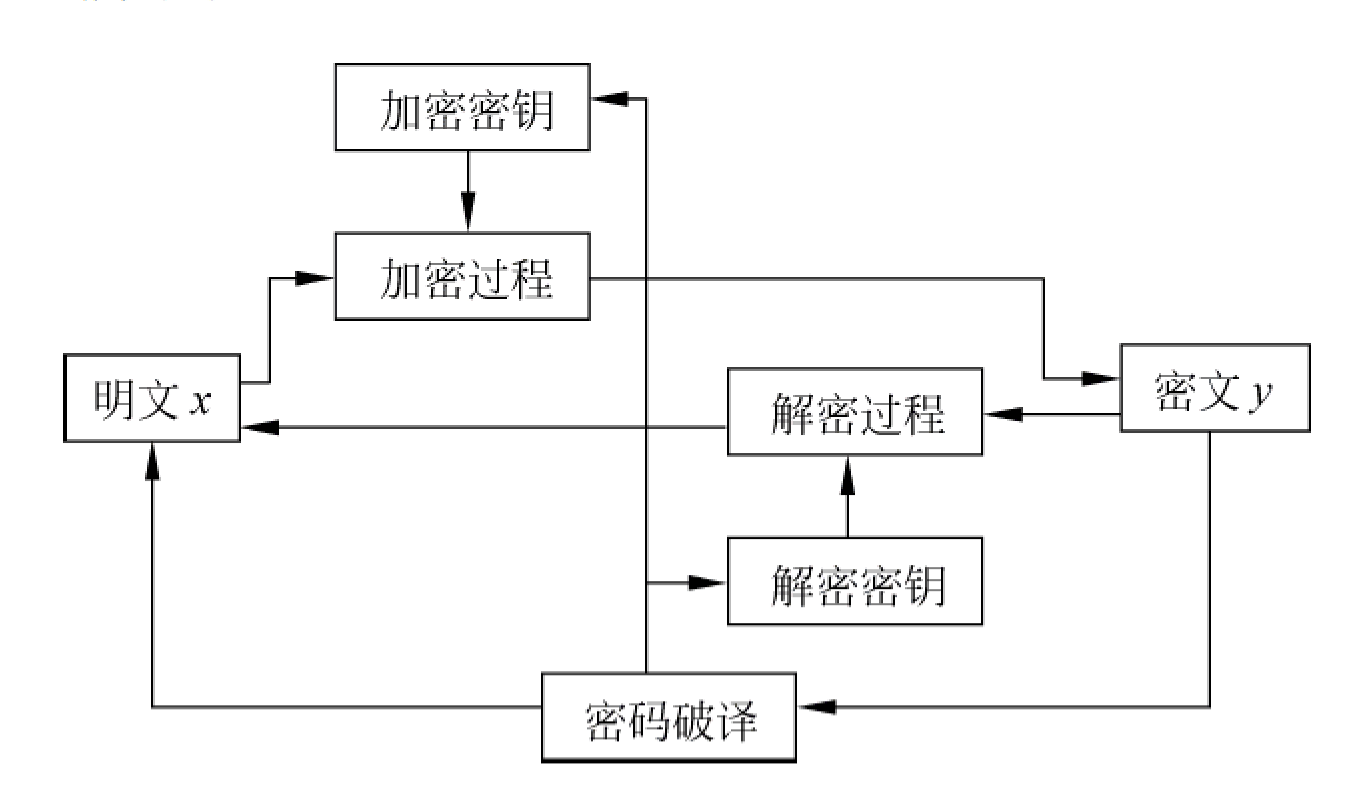


图 4.2　加密解密过程示意图

4.3　密 码 体 制

进行明密变换的法则，称为密码的体制。密码体制的基本类型可以分为四种：

(1) 错乱——按照规定的图形和线路，改变明文字母或数码等的位置成为密文；

(2) 代替——用一个或多个代替表将明文字母或数码等代替为密文；

(3) 密本——用预先编定的字母或数字密码组，代替一定的词组单词等变明文为密文；

(4) 加乱——用有限元素组成的一串序列作为乱数，按规定的算法，同明文序列相结合变成密文。

以上四种密码体制，既可单独使用，也可混合使用，以编制出各种复杂度很高的实用密码。

数据的加密和解密过程是通过密码体制＋密钥来控制的。密码体制必须易于使用，特别是应当可以在微型计算机上使用。密码体制的安全性依赖于密钥的安全性，现代密码学不追求加密算法的保密性，而是追求加密算法的完备，使攻击者在不知道密钥的情况下，没有办法从算法找到突破口。

密码学发展至今，已有两大类密码体制：第一类为对称密钥(单密钥)密码体制，第二类为非对称密钥(公共钥匙)密码体制。

4.3.1 对称密码体制

对称密码体制是一种传统密码体制，也称为私钥密码体制。在对称加密系统中，加密和解密采用相同的密钥。因为加、解密密钥相同，需要通信的双方必须选择和保存他们共同的密钥，各方必须信任对方不会将密钥泄密出去，这样就可以实现数据的机密性和完整性，如图 4.3 所示。

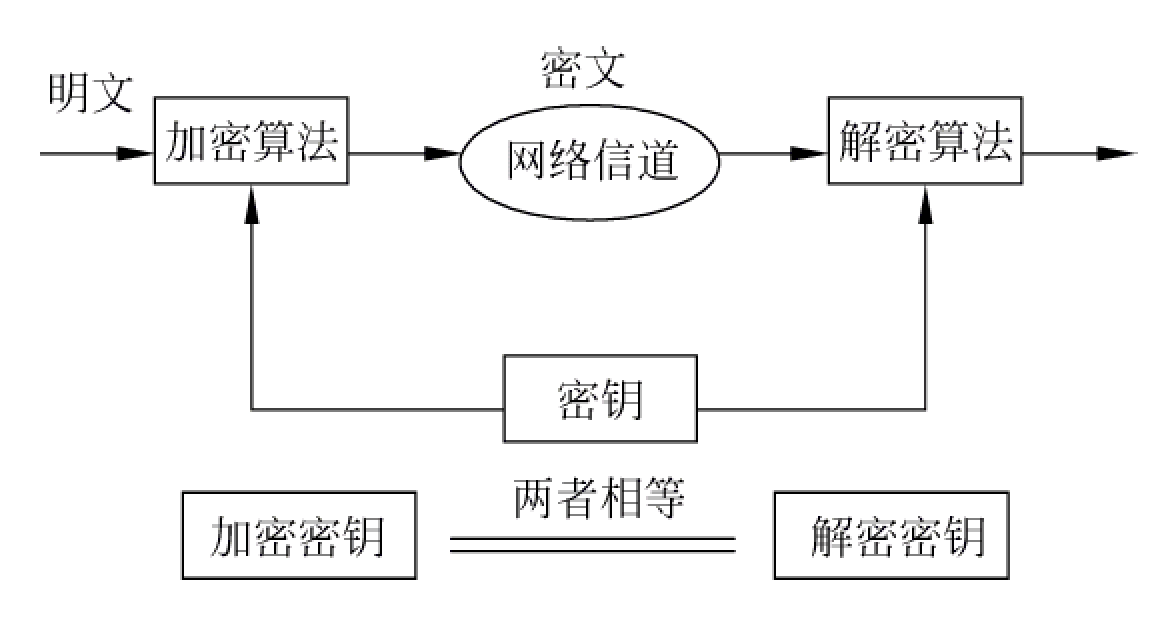


图 4.3 对称密码体制

对于具有 n 个用户的网络，需要 $n(n-1)/2$ 个密钥，在用户群不是很大的情况下，对称加密系统是有效的。但是对于大型网络，当用户群很大，分布很广时，密钥的分配和保存就成了问题。对机密信息进行加密和验证随报文一起发送报文摘要（或散列值）来实现。比较典型的算法有 DES 算法及其变形 Triple DES（三重 DES）、GDES（广义 DES），欧洲的 IDEA，日本的 FEAL N、RC5 等。DES 标准由美国国家标准局提出，主要应用于银行业的电子资金转账（EFT）领域。DES 的密钥长度为 56b。Triple DES 使用两个独立的 56b 密钥对交换的信息进行三次加密，从而使其有效长度达到 112b。RC2 和 RC4 方法是 RSA 数据安全公司的对称加密专利算法，它们采用可变密钥长度的算法。通过规定不同的密钥长度，C2 和 RC4 能够提高或降低安全的程度。对称密码算法的优点是计算开销小，加密速度快，是目前用于信息加密的主要算法。它的局限性在于，存在着通信的贸易双方之间确保密钥安全交换的问题。此外，某一贸易方有几个贸易关系，就要维护几个专用密钥。对称密码算法也没法鉴别贸易发起方或贸易最终方，因为贸易的双方的密钥相同。另外，由于对称加密系统仅能用于对数据进行加、解密处理，提供数据的机密性，不能用于数字签名。因而人们迫切需要寻找新的密码体制。

4.3.2 非对称密码体制

非对称密码体制也叫公钥加密技术，该技术就是针对私钥密码体制的缺陷提出来的。在公钥加密系统中，加密和解密是相对独立的，加密和解密会使用两把不同的密钥，加密密钥（公开密钥）向公众公开，谁都可以使用，解密密钥（秘密密钥）只有解密人自己知道，非法使用者根据公开的加密密钥无法推算出解密密钥，所以也被称为公钥密码体制，如图 4.4 所示。

如果一个人选择并公布了他的公钥，另外任何人都可以用这一公钥来加密传送给那个人的消息。私钥是秘密保存的，只有私钥的所有者才能利用私钥对密文进行解密。公钥密码体制的算法中最著名的代表是 RSA 系统，此外还有背包密码、McEliece 密码、Diffe_

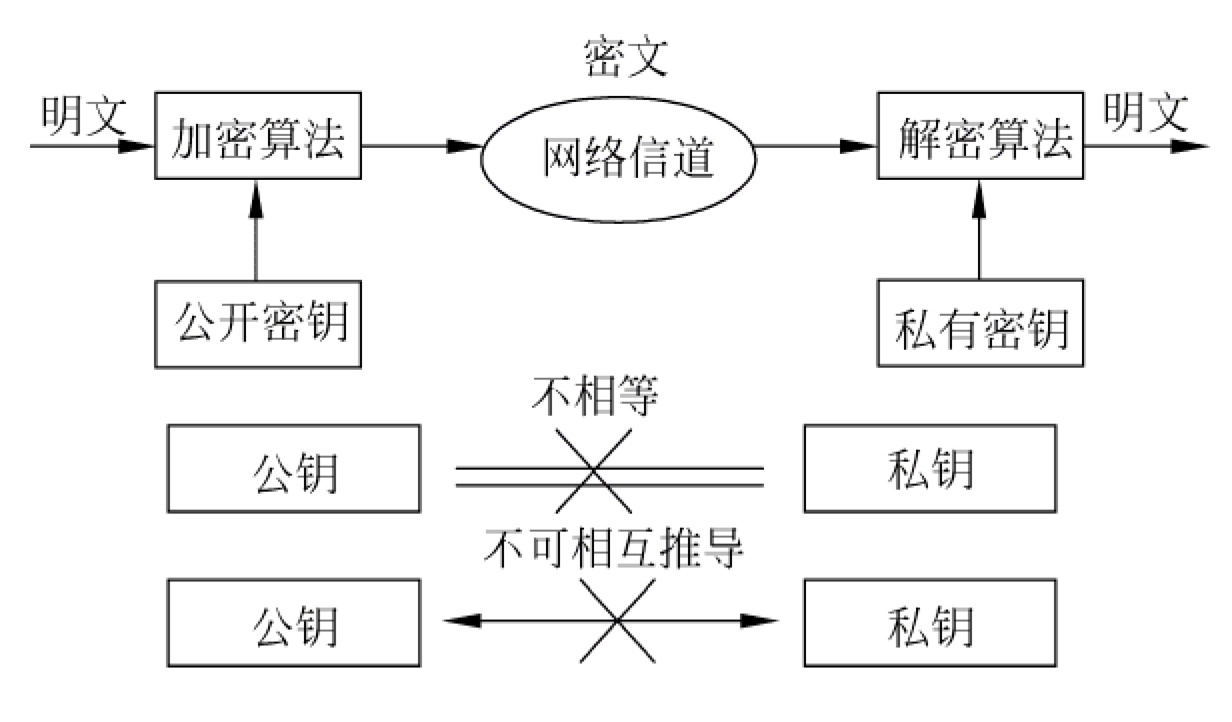


图 4.4　非对称密码体制

Hellman、Rabin、零知识证明、椭圆曲线、EIGamal 算法等。公钥密钥的密钥管理比较简单，并且可以方便地实现数字签名和验证。但算法复杂，加密数据的速率较低。公钥加密系统不存在对称加密系统中密钥的分配和保存问题，对于具有 n 个用户的网络，仅需要 $2n$ 个密钥。公钥加密系统除了用于数据加密外，还可用于数字签名。公钥加密系统可提供以下功能：

（1）机密性，保证非授权人员不能非法获取信息，通过数据加密来实现；

（2）确认性，保证对方属于所声称的实体，通过数字签名来实现；

（3）数据完整性，保证信息内容不被篡改，入侵者不可能用假消息代替合法消息，通过数字签名来实现；

（4）不可抵赖性，发送者不可能事后否认他发送过消息，消息的接收者可以向中立的第三方证实所指的发送者确实发出了消息，通过数字签名来实现。

可见公钥加密系统满足信息安全的所有主要目标。

4.4　哈希算法

哈希算法（hash algorithm），也叫信息标记算法（message-digest algorithm），可以提供数据完整性方面的判断依据。

哈希算法将任意长度的二进制值映射为固定长度的较小二进制值，这个小的二进制值称为哈希值。哈希值是一段数据唯一且极其紧凑的数值表示形式。如果散列一段明文而且哪怕只更改该段落的一个字母，随后的哈希都将产生不同的值。要找到散列为同一个值的两个不同的输入，在计算上是不可能的，所以数据的哈希值可以检验数据的完整性，流程如图 4.5 所示。

哈希表是根据设定的哈希函数和处理冲突方法将一组关键字映像到一个有限的地址区间上，并以关键字在地址区间中的像来记录表中的存储位置，这种表称为哈希表或散列，所得存储位置称为哈希地址或散列地址。作为线性数据结构与表格和队列等相比，哈希表无疑是查找速度比较快的一种。

哈希值通过将单向数学函数（有时称为“哈希算法”）应用到任意数量的数据所得到的固定大小的结果。如果输入数据中有变化，则哈希值也会发生变化。哈希值可用于许多操作，包括身份验证和数字签名，也称为“消息摘要”。

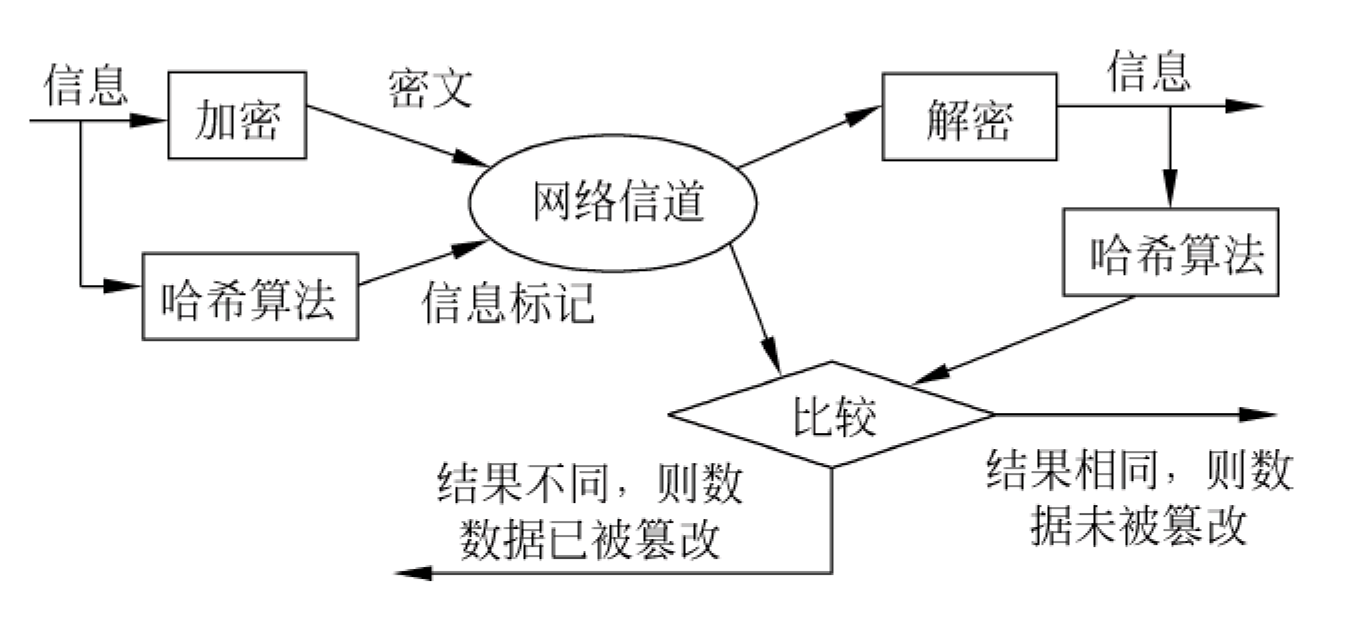


图 4.5　哈希(hash)算法

哈希算法是用来产生一些数据片段(例如消息或会话项)的哈希值的算法。使用好的哈希算法，在输入数据中所做的更改就可以更改结果哈希值中的所有位；因此，哈希对于检测数据对象(例如消息)中的修改很有用。此外，好的哈希算法使得构造两个相互独立且具有相同哈希的输入不能通过计算方法实现。典型的哈希算法包括 MD2、MD4、MD5 和 SHA-1。哈希算法也称为“哈希函数”。

哈希算法以一条信息为输入，输出一个固定长度的数字，称为“标记(digest)”。哈希算法具备三个特性：

(1) 不可能以信息标记为依据推导出输入信息的内容。

(2) 不可能人为控制某个消息与某个标记的对应关系(必须用 hash 算法得到)。

(3) 要想找到具有同样标记的信息在计算方面是行不通的。

哈希算法与加密算法共同使用，加强数据通信的安全性。采用这一技术的应用有数字签名、数字证书、网上交易、终端的安全连接、安全的电子邮件系统、PGP 加密软件等。

4.5　著名密码体系

4.5.1　分组密码体系

现代分组密码的研究始于 20 世纪 70 年代中期，至今已有 20 余年历史，这期间人们在这一研究领域已经取得了丰硕的研究成果。大体上，分组密码的研究包括三方面：分组密码的设计原理、分组密码的安全性分析和分组密码的统计性能测试。

分组密码的设计与分析是两个既相互对立又相互依存的研究方向，正是由于这种对立促进了分组密码的飞速发展。早期的研究基本上是围绕 DES 进行的，推出了许多类似于 DES 的密码，例如 LOKI、FEAL、GOST 等。进入 20 世纪 90 年代，人们对 DES 类密码的研究更加深入，特别是差分密码分析和线性密码分析的提出，迫使人们不得不研究新的密码结构。IDEA 密码的出现打破了 DES 类密码的垄断局面，IDEA 密码的设计思想是混合使用来自不同代数群中的运算。随后出现的 Square、Shark 和 Safer-64 都采用了结构非常清晰的代替-置换(SP)网络，每一轮由混淆层和扩散层组成。这种结构的最大优点是能够从理论上给出最大差分特征概率和最佳线性逼近优势的界，也就是密码对差分密码分析和线性密码分析是可证明安全的。

目前，对分组密码安全性的讨论主要包括差分密码分析、线性密码分析和强力攻击等。从理论上讲，差分密码分析和线性密码分析是目前攻击分组密码的最有效的方法，而从实际

上说，强力攻击是攻击分组密码最可靠的方法。到目前为止，已有大量文献讨论各种分组密码的安全性。自 AES（高级数据加密标准，是美国国家标准技术研究所旨在取代 DES 的 21 世纪的加密标准）候选算法公布以后，国内外许多专家都致力于候选算法的安全性分析，预计将会推出一些新的攻击方法，这无疑将进一步推动分组密码的发展。

与序列密码每次加密处理数据流的一位或一个字节不同，分组密码处理的单位是一组明文，即将明文消息编码后的数字序列 $x_0, x_1, x_2, \cdots, x_i$ 划分成长为 m 位的组 $x=(x_0, x_1, x_2, \cdots, x_{m-1})$，各个长为 m 的分组分别在密钥 $k=(k_0, k_1, k_2, \cdots, k_{m-1})$（密钥长为 m）的控制下变换成与明文组等长的一组密文输出数字序列 $y=(y_0, y_1, y_2, \cdots, y_{m-1})$。$m$ 通常为 64 或 128，原理如图 4.6 所示。

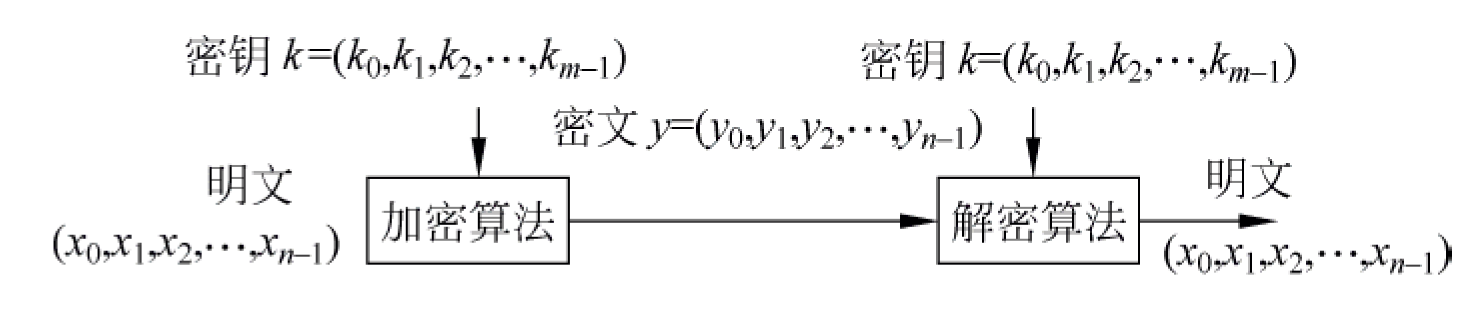


图 4.6　分组密码设计原理

分组密码算法实际上就是在密钥控制下，通过某个置换来实现对明文分组的加密变换。为了保证密码算法的安全强度，对密码算法的要求如下：

(1) 分组长度足够大。当分组长度较小时，分组密码类似于古典的代替密码，它仍然保留了明文的统计信息，这种统计信息将给攻击者留下可乘之机，攻击者可以有效地穷举明文空间，得到密码变换本身。

(2) 密钥量足够大。分组密码的密钥所确定密码变换只是所有置换中极小一部分。如果这一部分足够小，攻击者可以有效地穷举明文空间确定所有的置换。这时，攻击者就可以对密文进行解密，以得到有意义的明文。

(3) 密码变换足够复杂。使攻击者除了穷举法以外，找不到其他快捷的破译方法。

分组密码是将明文消息编码表示后的数字（简称明文数字）序列，划分成长度为 n 的组（可看成长度为 n 的矢量），每组分别在密钥的控制下变换成等长的输出数字（简称密文数字）序列。

分组密码将定长的明文块转换成等长的密文，这一过程在秘钥的控制之下。使用逆向变换和同一密钥来实现解密。对于当前的许多分组密码，分组大小是 64 位，但这很可能会增加。

明文消息通常要比特定的分组大小长得多，而且使用不同的技术或操作方式。这样的方式示例有电子编码本（ECB）、密码分组链接（CBC）或密码反馈（CFB）。ECB 使用同一个密钥简单地将明文块一个接一个地进行加密；在 CBC 方式中，每个明文块在加密前先与前一密文块进行"异或"运算，从而增加了复杂程度，可以使某些攻击更难以实施。"输出反馈"方式（OFB）类似 CBC 方式，但是进行"异或"的量是独立生成的。CBC 受到广泛使用，例如在 DES 实现中，而且在有关密码术的技术性方面的相应书籍中深入讨论了各种方式。请注意：有些用户自己建立的密码系统的普遍弱点就是以简单的形式来使用某些公开的算法，而不是以提供了额外保护的特定方式使用。

迭代的分组密码是那些其加密过程有多次循环的密码，因此提高了安全性。在每个循环中，可以通过使用特殊的函数从初始密钥派生出的子密钥来应用适当的变换。该附加的

计算需求必然会影响可以管理加密的速度,因此在安全性需要和执行速度之间存在着一种平衡。分组密码包括 DES、IDEA、SAFER、Blowfish 和 Skipjack(最后一个是“美国国家安全局”限制器芯片中使用的算法)。

4.5.2 DES 数据加密标准

在所有分组密码中,数据加密标准(DES)可谓是最著名的了。1973 年,美国国家标准局(NBS)在认识到建立数据保护标准既明显又急迫需要的情况下,开始征集联邦数据加密标准的方案。1975 年 3 月 17 日,NBS 公布了 IBM 公司提供的密码算法,以标准建议的形式在全国范围内征求意见。经过两年多的公开讨论之后,1977 年 7 月 15 日,NBS 宣布接受这个建议,作为联邦信息处理标准 46 号,数据加密标准即 DES 正式颁布,供商业界和非国防性政府部门使用。这是唯一由美国政府颁布的公开加密算法。

DES 密码在过去 20 年被正式作为国际标准采用,但业界认为其 56 位密钥太短,而且其基本设计原理,如各种不同排列选择、置换、叠代次数等没有清楚的说明,存在系统隐蔽陷阱的可能。

DES 是一种对二进制数据进行加密的算法。数据分组长为 64 位,密钥长也为 64 位。使用 56 位密钥对 64 位的数据块进行加密,并对 64 位的数据块进行 16 轮编码。在每轮编码时,一个 48 位的“每轮”密钥值由 56 位的完整密钥得出来。经过 16 轮的迭代、乘积变换、压缩变换等,输出密文也为 64 位。DES 算法的安全性完全依赖于其所用的密钥。

DES 用软件进行解码需要用很长时间,而用硬件解码速度非常快,但幸运的是当时大多数黑客并没有足够的设备制造出这种硬件设备。

在 1977 年,人们估计要耗资两千万美元才能建成一个专门计算机用于 DES 的解密,而且需要 12 个小时的破解才能得到结果,所以,当时 DES 被认为是一种十分强壮的加密方法。

1997 年开始,RSA 公司发起了一个称作“向 DES 挑战”的竞技赛。1997 年 1 月,用了 96 天时间,成功地破解了用 DES 加密的一段信息;一年之后,在第二届赛事上,这一记录为 41 天;1998 年 7 月,“第 2-2 届 DES 挑战赛(DES Challenge II-2)”把破解 DES 的时间缩短到了只需 56 小时;“第三届 DES 挑战赛(DES Challenge III)”把破解 DES 的时间缩短到了只需 22.5 小时。

4.5.3 公开密钥密码体制

公开密钥密码体制是现代密码学的最重要的发明和进展。一般理解密码学就是保护信息传递的机密性。但这仅仅是当今密码学主题的一个方面。对信息发送与接收人的真实身份的验证、对所发出/接收信息在事后的不可抵赖以及保障数据的完整性是现代密码学主题的另一方面。

公开密钥密码体制对这两方面的问题都给出了出色的解答,并正在继续产生许多新的思想和方案。在公钥体制中,加密密钥不同于解密密钥。人们将加密密钥公之于众,谁都可以使用;而解密密钥只有解密人自己知道。

公钥密码体制于 1976 年由 W. Diffie 和 M. Hellman 提出,同时,R. Merkle 也独立提出了这一体制。这种密码体制采用了一对密钥,即加密密钥和解密密钥(且从解密密钥推出

加密密钥是不可行的),这一对密钥中,一个可以公开(称为公钥),另一个为用户专用(私钥)。其原理是加密密钥和解密密钥分离。这样,一个具体用户就可以将自己设计的加密密钥和算法公诸于众,而只保密解密密钥。任何人利用这个加密密钥和算法向该用户发送的加密信息,该用户均可以将之还原。公开密钥密码的优点是不需要经安全渠道传递密钥,大大简化了密钥管理。它的算法有时也称为公开密钥算法或简称为公钥算法。

公钥密码体制可用于以下三个方面。

(1) 通信保密。此时将公钥作为加密密钥,私钥作为解密密钥,通信双方不需要交换密钥就可以实现保密通信。这时,通过公钥或密文分析出明文或私钥是不可行的。如图 4.7 所示,Bob 拥有多个人的公钥,当他需要向 Alice 发送机密消息时,他用 Alice 公布的公钥对明文消息加密,当 Alice 接收到后用她的私钥解密。由于私钥只有 Alice 本人知道,所以能实现通信保密。

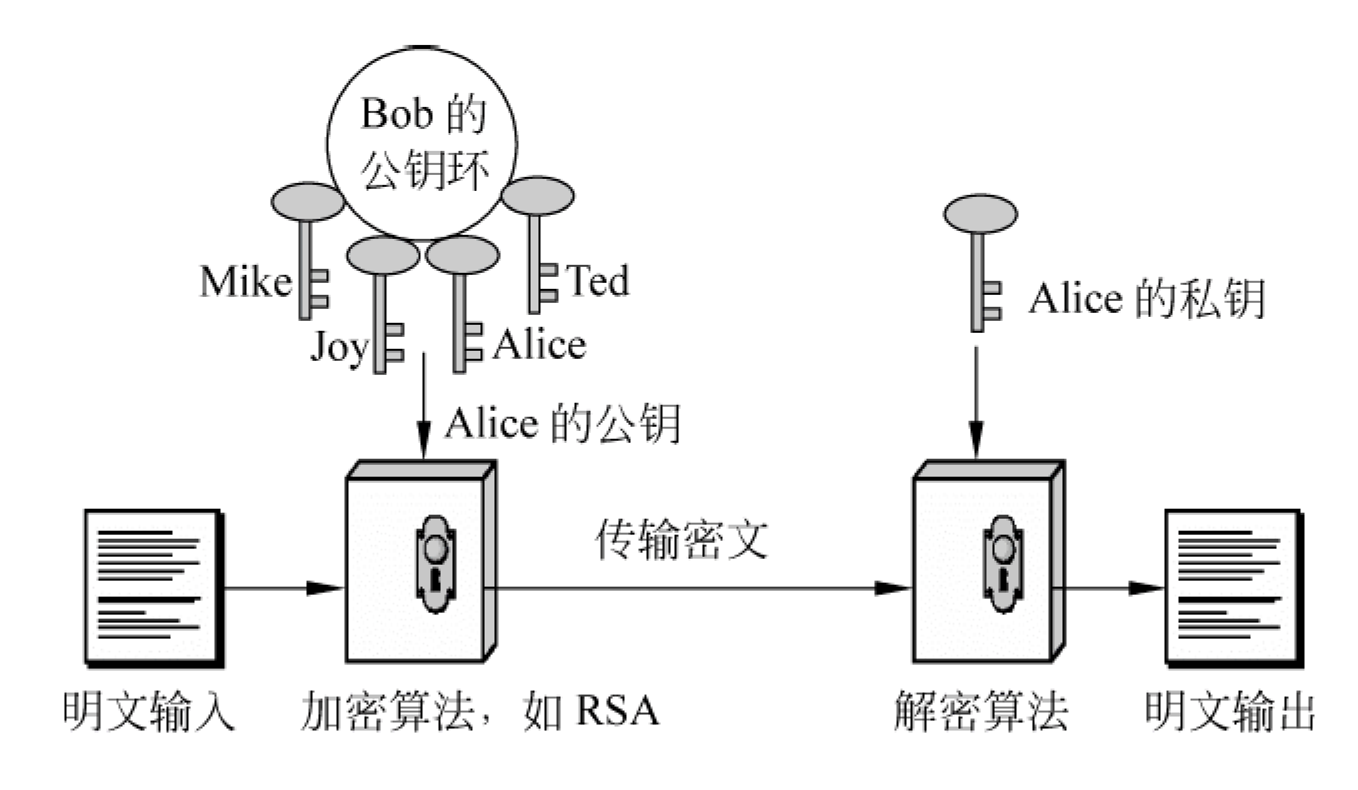


图 4.7　通信保密

(2) 数字签名。将私钥作为加密密钥,公钥作为解密密钥,可实现由一个用户对数据加密而使多个用户解读。如图 4.8 所示,Bob 用私钥对明文进行加密并发布,Alice 收到密文后用 Bob 公布的公钥解密。由于 Bob 的私钥只有 Bob 本人知道,因此,Alice 看到的明文肯定是 Bob 发出的,从而实现了数字签名。

(3) 密钥交换。通信双方交换会话密钥,以加密通信双方后续连接所传输的信息。每次逻辑连接使用一把新的会话密钥,用完就丢弃。

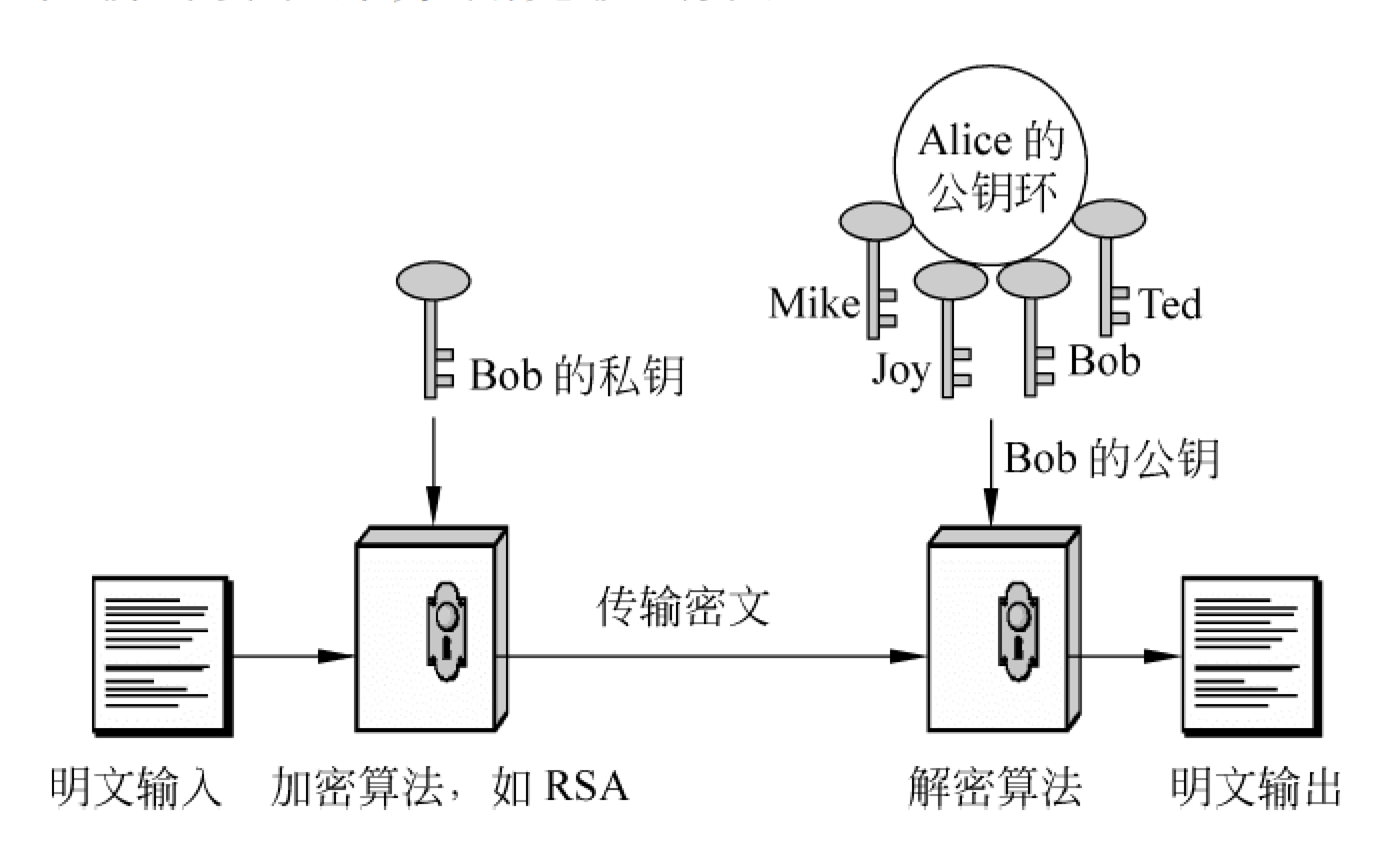


图 4.8　数字签名

4.5.4 公开密钥算法

迄今为止的所有公钥密码体系中，公开密钥算法(RSA)系统是最著名、使用最广泛的一种。RSA 是 1977 年由 MIT 教授 Ronald L. Rivest、Adi Shamir 和 Leonard M. Adleman 共同开发的，分别取三名数学家名字的第一个字母来构成的。

RSA 使用两个密钥，一个公开密钥，一个专用密钥。如用其中一个加密，则可用另一个解密，密钥长度从 40 到 2048b 可变，加密时也把明文分成块，块的大小可变，但不能超过密钥的长度，RSA 算法把每一块明文转化为与密钥长度相同的密文块。密钥越长，加密效果越好，但加密解密的开销也大，所以要在安全与性能之间折中考虑，一般 64 位是较合适的。RSA 的一个比较知名的应用是 SSL，在美国和加拿大 SSL 用 128 位 RSA 算法，由于出口限制，在其他地区(包括中国)通用的则是 40 位版本。

RSA 算法研制的最初理念与目标是努力使互联网安全可靠，旨在解决 DES 算法密钥利用公开信道传输分发的难题。而实际结果不但很好地解决了这个难题；还可利用 RSA 来完成对电文的数字签名以对抗电文的否认与抵赖；同时还可以利用数字签名较容易地发现攻击者对电文的非法篡改，以保护数据信息的完整性。

RSA 算法的安全性基于大数分解的困难性。我们知道，求一对大素数的乘积很容易，但要对这个乘积进行因式分解则非常困难，因此，可以把一对大素数的乘积公开作为公钥，而把素数作为私钥，从而从一个公开密钥和密文中恢复出明文的难度等价于分解两个大素数之积。

RSA 算法很好地完成了对电文的数字签名以对抗数据的否认与抵赖。利用数字签名较容易地发现攻击者对电文的非法篡改，以保护数据信息的完整性。目前为止，很多种加密技术采用了 RSA 算法，比如 PGP(PrettyGoodPrivacy)加密系统，它是一个工具软件，向认证中心注册后就可以用它对文件进行加解密或数字签名。由此可以看出 RSA 有很好的应用，是迄今理论上最为成熟完善的一种公钥密码体制。

RSA 密码基于计算复杂性原理获得加密强度，但其缺点是系统的安全取决于所用的两个大素数，如果能找出一种快速方法分解这两个大素数，系统很容易被攻破。

RSA 的安全性是比较高的，就目前的计算机水平用 1024 位的密钥是安全的，2048 位是绝对安全的。RSA 实验室认为，512 位的密钥已不够安全，应停止使用，现在的个人需要用 668 位的密钥，公司要用 1024 位的密钥，极其重要的场合应该用 2048 位的密钥。

公开密钥方案较对称密钥方案处理速度慢，因此，通常把公开密钥与对称密钥技术结合起来以实现最佳性能。即用公开密钥技术在通信双方之间传送对称密钥，而用对称密钥来对实际传输的数据加密解密。另外，公钥加密也用来对对称密钥进行加密。

4.6 PGP 加密软件

PGP，全称 Pretty Good Privacy，是一种在信息安全传输领域首选的加密软件，其技术特性是采用了非对称的公钥加密体系。由于美国对信息加密产品有严格的法律约束，特别是对向美国、加拿大之外国家散播该类信息，以及出售、发布该类软件约束更为严格。因而限制了 PGP 的一些发展和普及，现在该软件的主要使用对象为情报机构、政府机构、信息安

全工作者(例如较有水平的安全专家和有一定资历的黑客)。PGP 最初的设计主要是用于邮件加密,如今已经发展到了可以加密整个硬盘、分区、文件、文件夹、集成进邮件软件进行邮件加密,甚至可以对 ICQ 的聊天信息实时加密。聊天者只要安装了 PGP,就可利用其 ICQ 加密组件在双方聊天的同时进行加密或解密,最大程度地保证聊天信息不被窃取或监视。

PGP 使用加密以及效验的方式,提供了多种的功能和工具,帮助保证电子邮件、文件、磁盘以及网络通信的安全。

(1) 在任何软件中进行加密/签名以及解密/效验。通过 PGP 选项和电子邮件插件,可以在任何软件当中使用 PGP 的功能。

(2) 创建以及管理密钥。使用 PGPkeys 来创建、查看和维护自己的 PGP 密钥对;以及把任何人的公钥加入自己的公钥库中。

(3) 创建自解密压缩文档。可以建立一个自动解密的可执行文件。任何人不需要事先安装 PGP,只要得知该文件的加密密码,就可以把这个文件解密。这个功能尤其在需要把文件发送给没有安装 PGP 的人时特别好用。并且,此功能还能对内嵌其中的文件进行压缩,压缩率与 ZIP 相似,比 RAR 略低(某些时候略高,比如含有大量文本)。总的来说,该功能是相当出色的。

(4) 创建 PGPdisk 加密文件。该功能可以创建一个. pgd 文件,此文件用 PGP Disk 功能加载后,将以新分区的形式出现,可以在此分区内放入需要保密的任何文件。其使用私钥和密码两者共用的方式保存加密数据,保密性坚不可摧,但需要注意的是,一定要在重装系统前记得备份"我的文档"中的 PGP 文件夹里的所有文件,以备重装后恢复自己的私钥。该步骤一定不能漏掉,否则将永远没有可能再次打开曾经在该系统下创建的任何加密文件!

(5) 永久地粉碎销毁文件、文件夹,并释放出磁盘空间。可以使用 PGP 粉碎工具来永久地删除那些敏感的文件和文件夹,而不会遗留任何的数据片段在硬盘上。也可以使用 PGP 自由空间粉碎器来再次清除已经被删除的文件实际占用的硬盘空间。这两个工具都是要确保所删除的数据将永远不可能被别有用心的人恢复。

(6) 9. x 新增:全盘加密,也称完整磁盘加密。该功能可将整个硬盘上所有数据加密,甚至包括操作系统本身。提供极高的安全性,没有密码之人绝无可能使用加密过的系统或查看硬盘里面存放的文件、文件夹等数据。即便是硬盘被拆卸到另外的计算机上,该功能仍将忠实地保护被加密的数据,加密后的数据维持原有的结构,文件和文件夹的位置都不会改变。

(7) 9. x 增强:即时消息工具加密。该功能可将支持的即时消息工具所发送的信息完全经由 PGP 处理,只有拥有对应私钥和密码的对方才可以解开消息的内容。任何人截获到也没有任何意义,仅仅是一堆乱码。

(8) 9. x 新增:PGP zip,PGP 压缩包。该功能可以创建类似其他压缩软件打包压缩后的文件包,但不同的是其拥有坚不可摧的安全性。

(9) 9. x 增强:网络共享。可以使用 PGP 接管共享文件夹本身以及其中的文件,安全性远远高于操作系统本身提供的账号验证功能。并且可以方便地管理允许的授权用户可以进行的操作。极大地方便了需要经常在内部网络中共享文件的企业用户,使他们免受蠕虫病毒和黑客的侵袭。

4.6.1 PGP的技术原理

PGP加密系统是采用公开密钥加密与传统密钥加密相结合的一种加密技术。它使用一对数学上相关的钥匙,其中一个(公钥)用来加密信息,另一个(私钥)用来解密信息。

PGP采用的传统加密技术部分所使用的密钥称为“会话密钥”(sek)。每次使用时,PGP都随机产生一个128位的IDEA会话密钥,用来加密报文。公开密钥加密技术中的公钥和私钥则用来加密会话密钥,并通过它间接地保护报文内容。

PGP中的每个公钥和私钥都伴随着一个密钥证书。它一般包含以下内容:

(1)密钥内容(用长达百位的大数字表示的密钥);

(2)密钥类型(表示该密钥为公钥还是私钥);

(3)密钥长度(密钥的长度,以二进制位表示);

(4)密钥编号(用以唯一标识该密钥);

(5)创建时间;

(6)用户标识(密钥创建人的信息,如姓名、电子邮件等);

(7)密钥指纹(为128位的数字,是密钥内容的提要,表示密钥唯一的特征);

(8)中介人签名(中介人的数字签名,声明该密钥及其所有者的真实性,包括中介人的密钥编号和标识信息)。

PGP把公钥和私钥存放在密钥环(KEYR)文件中。PGP提供有效的算法查找用户需要的密钥。PGP在多处需要用到口令,它主要起到保护私钥的作用。由于私钥太长且无规律,所以难以记忆。PGP把它用口令加密后存入密钥环,这样用户可以用易记的口令间接使用私钥。

PGP的每个私钥都由一个相应的口令加密。PGP主要在三处需要用户输入口令:

(1)需要解开收到的加密信息时,PGP需要用户输入口令,取出私钥解密信息;

(2)当用户需要为文件或信息签字时,用户输入口令,取出私钥加密;

(3)对磁盘上的文件进行传统加密时,需要用户输入口令。

4.6.2 PGP的密钥管理

PGP使用了四种类型的密钥:一次性会话对称密钥、公钥、私钥和基于口令短语的对称密钥。

(1)会话密钥,使用CAST-128算法本身来产生随机的128比特数字。将128比特的密钥和两个作为明文的64比特块作为输入,CAST-128算法用密码反馈模式加密这两个64比特块,并将密文块连接起来形成128比特的会话密钥。两个作为明文输入到随机数发生器的64比特块来自于128比特的随机数据流。这个随机数据流的产生是以用户的击键为基础的,击键时间和键值用于产生随机数据流。

(2)密钥标识符,在PGP中,加密的消息与加密的会话密钥一起发送给消息的接收者。会话密钥是使用接收者的公钥加密的,因此,只有接收者才能够恢复会话密钥,从而解密消息。如果接收者只有一个公钥/私钥对,接收者就会自动知道用哪个密钥来解密会话密钥。但如上所述,一个用户可能拥有多个公钥/私钥对,这种情况下,接收者如何知道会话密钥是使用哪个公钥加密的呢?一个简单的办法就是:消息的发送者将加密会话密钥的公钥与消

息一起传过去，接收者验证收到的公钥确实是自己的以后，进行解密操作。但这样做会造成空间的浪费，因为 RSA 的密钥很大，可能由几百个十进位组成。

PGP 采用的解决办法是为每个公钥分配一个密钥 ID，并且很有可能这个密钥 ID 在用户 ID 内是唯一的。与每个公钥关联的密钥 ID 包含公钥的低 64 位。这个长度足以保证密钥发生重复的概率非常小。详细的使用操作请参见第 13 章。

4.7 软件与硬件加密技术

4.7.1 软件加密

软件加密一般是用户在发送信息前，先调用信息安全模块对信息进行加密，然后发送，到达接收方后，由用户使用相应的解密软件进行解密并还原。软件加密的方法有密码表加密、软件子校验方式、序列号加密、许可证管理方式、钥匙盘方式、光盘加密等。

1. 序列号加密

现今很多共享软件大多采用这种加密方式，用户在软件的试用期是不需要交费的，一旦试用期满还希望继续使用这个软件，就必须到软件公司进行注册，然后软件公司会根据用户提交的信息(一般是用户的名字)来生成一个序列号，当收到这个序列号以后，并在软件运行的时候输入进去，软件会验证用户的名字与序列号之间的关系是否正确，如果正确说明用户已经购买了这个软件，也就没有日期的限制了。

2. 许可证加密

许可证加密是序列号加密的一个变种。从网上下载或购买的软件并不能直接使用，软件在安装时或运行时会对用户的计算机进行一番检测，并根据检测结果生成一个特定指纹，这个指纹是一个数据文件，把这个指纹数据通过 Internet、E-mail、电话、传真等方式发送到开发商那里，开发商再根据这个指纹给用户一个注册码或注册文件，用户得到这个注册码或注册文件并按软件要求的步骤在自己的计算机上完成注册后方能使用。

但是采用软件加密方式，有一些安全隐患：

(1) 密钥的管理很复杂，这也是安全 API 实现的一个难题，从目前的几个 API 产品来讲，密钥分配协议均有缺陷；

(2) 使用软件加密，因为是在用户的计算机内部进行，容易让攻击者采用跟踪、反编译等手段进行攻击；

(3) 目前国内尚无自己的安全 API 产品，另外软件加密速度相对较慢。

4.7.2 硬件加密

硬件加密则是采用硬件(电路、器件、部件等)和软件结合来实现的加密，对硬件本身和软件采取加密、隐藏、防护技术，防止被保护对象被攻击者破析、破译。硬件加解密是商业或军事上的主流，硬件加密的方法有加密卡、软件狗和微狗等。硬件加密具有以下几个特点。

(1) 速度问题：针对位的操作、不占用计算机主处理器。

(2) 安全性：可进行物理保护，由硬件完成加密解密和权限检查，防止破译者通过反汇

编、反编译分析破译。

(3) 易于安装：无须使用计算机的电话、传真、数据线路；计算机环境下，使用硬件加密可对用户透明；软件实现，需要在操作系统深层安装，不容易实现。

(4) 在硬件内设置自毁装置，一旦发现硬件被拆卸或程序被跟踪，促使硬件自毁，使破译者不敢进行动态跟踪。

硬件加密是目前广泛采用的加密手段，加密后软件执行时需访问相应的硬件，如插在计算机扩展槽上的卡或插在计算机并口上的“狗”。采用硬件加密的软件执行时需和相应的硬件交换数据，若没有相应的硬件，加密后的软件将无法执行。

4.8 数字签名与数字证书

4.8.1 数字签名

所谓数字签名就是附加在数据单元上的一些数据，或是对数据单元所做的密码变换。这种数据或变换，允许数据单元的接收者用以确认数据单元的来源和数据单元的完整性并保护数据，防止被人(例如接收者)进行伪造。它是对电子形式的消息进行签名的一种方法，一个签名消息能在一个通信网络中传输。基于公钥密码体制和私钥密码体制都可以获得数字签名，目前主要是基于公钥密码体制的数字签名。包括普通数字签名和特殊数字签名。普通数字签名算法有 RSA、ElGamal、Fiat-Shamir、Guillou- Quisquarter、Schnorr、Ong-Schnorr-Shamir 数字签名算法、Des/DSA，椭圆曲线数字签名算法和有限自动机数字签名算法等。特殊数字签名有盲签名、代理签名、群签名、不可否认签名、公平盲签名、门限签名、具有消息恢复功能的签名等，它与具体应用环境密切相关。显然，数字签名的应用涉及法律问题，美国联邦政府基于有限域上的离散对数问题制定了自己的数字签名标准(DSS)。

数字签名技术是不对称加密算法的典型应用。数字签名的应用过程是，数据源发送方使用自己的私钥对数据校验和其他与数据内容有关的变量进行加密处理，完成对数据的合法“签名”；数据接收方则利用对方的公钥来解读收到的“数字签名”，并将解读结果用于对数据完整性的检验，以确认签名的合法性。数字签名技术是在网络系统虚拟环境中确认身份的重要技术，完全可以代替现实过程中的“亲笔签字”，在技术和法律上有保证。在公钥与私钥管理方面，数字签名应用与加密邮件 PGP 技术正好相反。在数字签名应用中，发送者的公钥可以很方便地得到，但他的私钥则需要严格保密。

数字签名主要的功能是：保证信息传输的完整性、发送者的身份认证、防止交易中的抵赖发生。

数字签名技术是将摘要信息用发送者的私钥加密，与原文一起传送给接收者。接收者只有用发送的公钥才能解密被加密的摘要信息，然后用哈希函数对收到的原文产生一个摘要信息，与解密的摘要信息对比。如果相同，则说明收到的信息是完整的，在传输过程中没有被修改，否则说明信息被修改过，因此数字签名能够验证信息的完整性。

假定 A 需要传送一份合同给 B，B 需要确认合同的确是 A 发送的，同时还需要确定合同在传输途中未被修改。

通过比较标记 1 和标记 2，就可以确认合同是否是 A 发送的以及合同在传输途中是否

被修改,工作流程如图 4.9 所示。

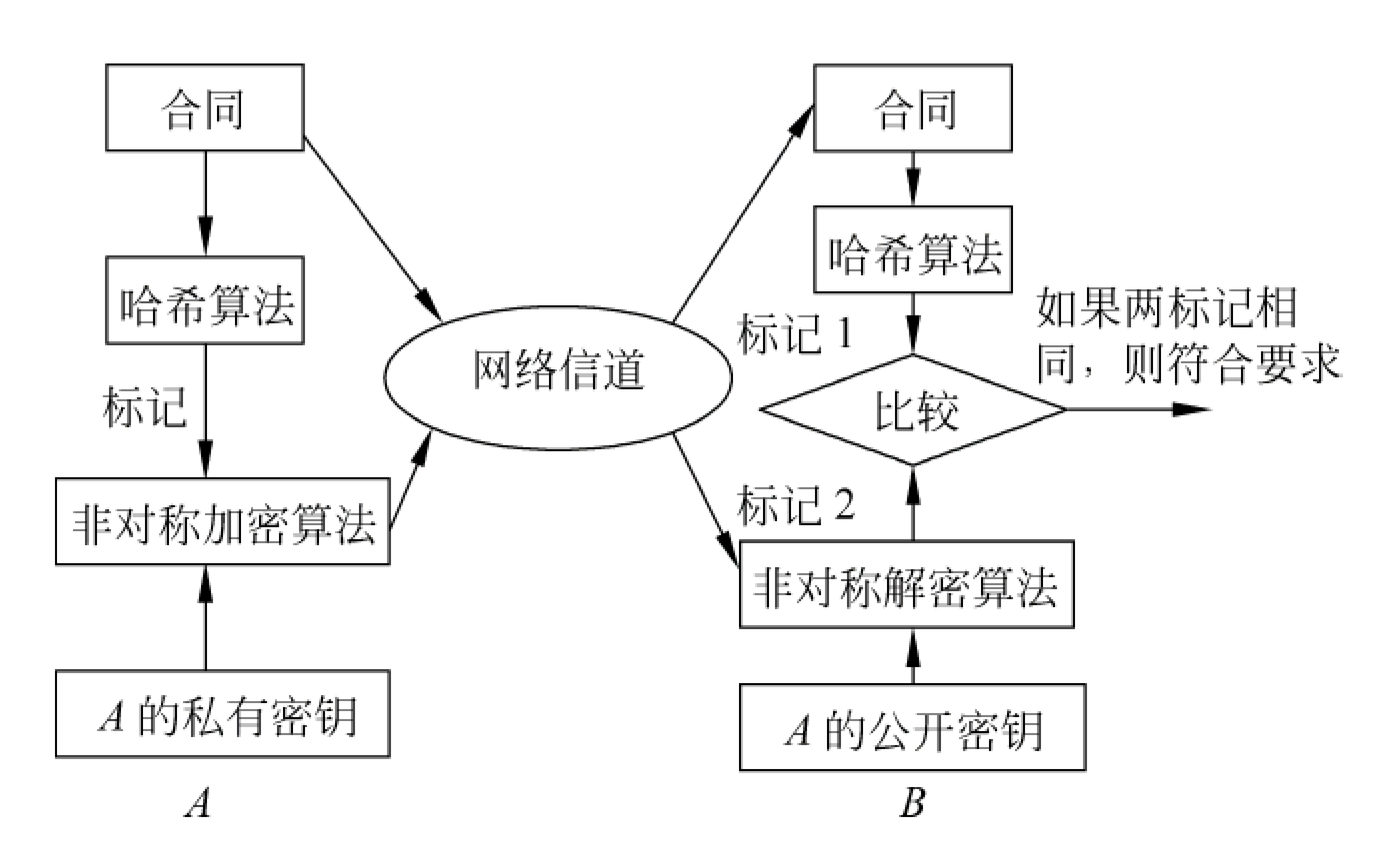


图 4.9　数字签名的工作流程

4.8.2　数字证书

当人们对签名人同公开密钥的对应关系产生疑问时,需要第三方颁证机构证书认证中心(Certificate Authorities,CA)的帮助。

由于电子商务技术使在网上购物的顾客能够极其方便地获得商家和企业的信息,但同时也增加了某些敏感或有价值的数据被滥用的风险。为了保证互联网上电子交易及支付的安全性和保密性,防范交易及支付过程中的欺诈行为,必须在网上建立一种信任机制。这就要求参加电子商务的买方和卖方都必须拥有合法的身份,并且在网上能够有效无误地被验证。数字证书是一种权威性的电子文档,它提供了一种在 Internet 上验证身份的方式,其作用类似于司机的驾驶执照或日常生活中的身份证。它是由权威机构 CA 证书授权中心发行的,人们可以在互联网交往中用它来识别对方的身份。当然在数字证书认证的过程中,证书认证中心(CA)作为权威的、公正的、可信赖的第三方,其作用是至关重要的。

数字证书也必须具有唯一性和可靠性。为了达到这一目的,需要采用很多技术来实现。通常,数字证书采用公钥体制,即利用一对互相匹配的密钥进行加密、解密。每个用户自己设定一把特定的仅为本人所有的私钥,用它进行解密和签名;同时设定一把公钥并由本人公开,为一组用户所共享,用于加密和验证签名。当发送一份保密文件时,发送方使用接收方的公钥对数据加密,而接收方则使用自己的私钥解密,这样信息就可以安全无误地到达目的地了。通过数字的手段保证加密过程是一个不可逆过程,即只有用私有密钥才能解密。公开密钥技术解决了密钥发布的管理问题,用户可以公开其公开密钥,而保留其私有密钥。

数字证书使用过程一般如图 4.10 所示,用户首先向 CA 机构申请一份数字证书,申请过程会生成他的公开/私有密钥对。公开密钥被发送给 CA 机构,CA 机构生成证书,并用自己的私有密钥签发,同时向用户发送一份备份。用户用数字证书把文件加上签名,然后把原始文件同签名一起发送给自己的同事。用户的同事从 CA 机构查到用户的数字证书,用证书中的公开密钥对签名进行验证。

基于数字证书的应用角度分类,数字证书可以分为以下几种。

1. 服务器证书

服务器证书被安装于服务器设备上,用来证明服务器的身份和进行通信加密。服务器

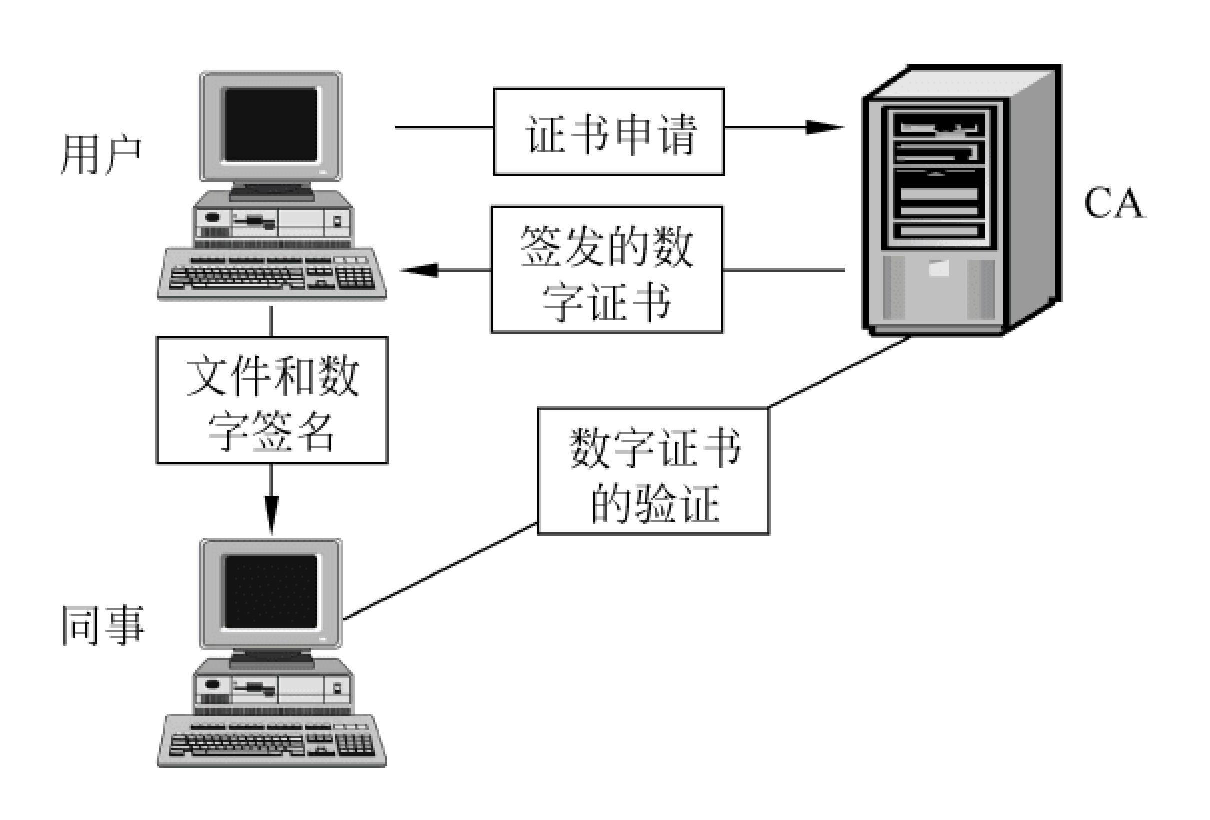


图 4.10　数字证书的使用过程

证书可以用来防止假冒站点。

在服务器上安装服务器证书后，客户端浏览器可以与服务器证书建立 SSL 连接，在 SSL 连接上传输的任何数据都会被加密。同时，浏览器会自动验证服务器证书是否有效，验证所访问的站点是否是假冒站点。服务器证书保护的站点多被用来进行密码登录、订单处理、网上银行交易等。全球知名的服务器证书品牌是 verisign、thawte、geotrust 等，其服务器证书编制起来的可信网络已覆盖全球。

SSL 证书主要用于服务器的数据传输链路加密和身份认证，绑定网站域名，不同的产品对于不同价值的数据和要求不同的身份认证。超真 SSL 和超快 SSL 在颁发时间上已经没有什么区别，主要区别在于：超快 SSL 只验证域名所有权，证书中不显示单位名称；而超真 SSL 需要验证域名所有权、营业执照和第三方数据库验证，证书中显示单位名称。

2. 电子邮件证书

电子邮件证书可以用来证明电子邮件发件人的真实性。它并不证明数字证书上面 CN 一项所标识的证书所有者姓名的真实性，它只证明邮件地址的真实性。

收到具有有效电子签名的电子邮件，我们除了能相信邮件确实由指定邮箱发出外，还可以确信该邮件从被发出后没有被篡改过。

另外，使用接收的邮件证书，我们还可以向接收方发送加密邮件。该加密邮件可以在非安全网络传输，只有接收方的持有者才可能打开该邮件。

3. 客户端个人证书

客户端证书主要被用来进行身份验证和电子签名。安全的客户端证书被存储于专用的 usbkey 中。存储于 key 中的证书不能被导出或复制，且 key 使用时需要输入 key 的保护密码。使用该证书需要物理上获得其存储介质 usbkey，且需要知道 key 的保护密码，这也被称为双因子认证。这种认证手段是目前在 Internet 最安全的身份认证手段之一。

客户端证书分超真单位证书、超真个人证书、超快个人证书、PDF 文件签名证书等。

数字证书相当于电子化的身份证明，应有值得信赖的颁证机构(CA 机构)的数字签名，可以用来强力验证某个用户或某个系统的身份及其公开密钥。

数字证书既可以向一家公共的办证机构申请，也可以向运转在企业内部的证书服务器申请。这些机构提供证书的签发和失效证明服务。

4.9 PKI 基础知识

PKI(Public Key Infrastructure)即“公开密钥体系”,是一种遵循既定标准的密钥管理平台,它能够为所有网络应用提供加密和数字签名等密码服务及所必需的密钥和证书管理体系,简单来说,PKI 就是利用公钥理论和技术建立的提供安全服务的基础设施。PKI 技术是信息安全技术的核心,也是电子商务的关键和基础技术。

4.9.1 PKI 的基本组成

完整的 PKI 系统必须具有权威认证机构(CA)、数字证书库、密钥备份及恢复系统、证书作废系统、应用接口(API)等基本构成部分,构建 PKI 也将围绕着这五大系统来着手构建。

(1) 认证机构,即数字证书的申请及签发机关,CA 必须具备权威性的特征。

(2) 数字证书库,用于存储已签发的数字证书及公钥,用户可由此获得所需的其他用户的证书及公钥。

(3) 密钥备份及恢复系统,如果用户丢失了用于解密数据的密钥,则数据将无法被解密,这将造成合法数据丢失。为避免这种情况,PKI 提供备份与恢复密钥的机制。但须注意,密钥的备份与恢复必须由可信的机构来完成。并且,密钥备份与恢复只能针对解密密钥,签名私钥为确保其唯一性而不能够作备份。

(4) 证书作废系统,是 PKI 的一个必备的组件。与日常生活中的各种身份证件一样,证书有效期以内也可能需要作废,原因可能是密钥介质丢失或用户身份变更等。为实现这一点,PKI 必须提供作废证书的一系列机制。

(5) 应用接口,PKI 的价值在于使用户能够方便地使用加密、数字签名等安全服务,因此一个完整的 PKI 必须提供良好的应用接口系统,使得各种各样的应用能够以安全、一致、可信的方式与 PKI 交互,确保安全网络环境的完整性和易用性。

4.9.2 PKI 的安全服务功能

为网上金融、网上银行、网上证券、电子商务、电子政务、网上交税、网上工商等多种网上办公、交易提供完备的安全服务功能,是公钥基础设施最基本、最核心的功能。PKI 体系作为基础设施要做到:遵循必要的原则,不同的实体可以方便地使用 PKI 安全基础设施提供的服务。安全服务功能包括身份认证、完整性、机密性、不可否认性、时间戳和数据的公正性服务。

1. 网上身份安全认证

由于网络使用者匿名的特点,每个人都可以通过一定的手段假冒别人的身份实施非法的操作和网上交易,从而对系统或合法用户造成危害,因此,网上的身份认证在网络出现以来就一直是人们关注和研究的热点。人们已经认识到网上身份认证是一切电子商务应用的基础。

认证的实质就是证实被认证对象是否属实和是否有效的过程,常常被用于通信双方相互确认身份,以保证通信的安全。其基本思想是通过验证被认证对象的某个专有属性,达到确认被认证对象是否真实、有效的目的。被认证对象的属性可以是口令、数字签名或者指

纹、声音、视网膜这样的生理特征等。目前,实现认证的技术手段很多,通常有口令技术加ID(实体唯一标识)、双因素认证、挑战应答式认证、著名的Kerberos认证系统,以及X.509证书及认证框架。这些不同的认证方法所提供的安全认证强度也不一样,具有各自的优势、不足,以及所适用的安全强度要求不同的应用环境。而解决网上电子身份认证的PKI技术近年来被广泛应用,并取得了飞速的发展,在网上银行、电子政务等保护用户信息资产等领域发挥了巨大的作用。

数字签名技术是基于公钥密码学的强认证技术,其中每个参与交易的实体都拥有一对签名的密钥。每个参与的交易者都自己掌握进行签名的私钥,私钥不在网上传输,因此只有签名者自己知道签名私钥,从而保证其安全。公开的是进行验证签名的公钥。因此只要私钥安全,就可以有效地对产生该签名的声称者进行身份验证,保证交互双方的身份真实性。

为了保证公钥的可靠性,即保证公钥与其拥有者的有效绑定,通过PKI体系中的权威、公正的第三方——认证中心(CA),为所服务的PKI域内的相关实体签发一个网上身份证即数字证书,来保证公钥的可靠性,以及它与合法用户的对应关系。数字证书中主要包含的就是证书所有者的信息、证书所有者的公开密钥和证书颁发机构的签名,以及有关的扩展内容等。具备了这些条件,就可以在具体的业务中有效实现交易双方的身份认证。

2. 保证数据完整性

数据的完整性就是防止非法篡改信息,如修改、复制、插入、删除等。在交易过程中,要确保交易双方接收到的数据和从数据源发出的数据完全一致,数据在传输和存储的过程中不能被篡改,否则交易将无法完成或所做交易违背交易意图。

但直接观察原始数据的状态来判断其是否改变,在很多情况下是不可行的。如果数据量很大,将很难判断其是否被篡改,即完整性很难得到保证。为了保证数据的完整性,已出现了各种不同的安全机制和方法。其中在电子商务和网络安全领域使用最多的就是密码学为我们提供的数据完整性机制和方法。

在国内PKI体系所实现的方案中,目前采用的标准散列算法有SHA-1、MD-5作为可选的Hash算法来保证数据的完整性。在实际应用中,通信双方通过协商以确定使用的算法和密钥,从而在两端计算条件一致的情况下,对同一数据应当计算出相同的算法来保证数据不被篡改,实现数据的完整性。

3. 保证网上交易的抗否认性

不可否认用于从技术上保证实体对他们行为的诚实,即参与交互的双方都不能事后否认自己曾经处理过的每笔业务。在这中间,人们更关注的是数据来源的不可否认性、发送方的不可否认性,以及接收方在接收后的不可否认性。此外,还有传输的不可否认性、创建的不可否认性和同意的不可否认性等。PKI所提供的不可否认功能,是基于数字签名以及其所提供的时间戳服务功能的。

在进行数字签名时,签名私钥只能被签名者自己掌握,系统中的其他参与实体无法得到该密钥,这样只有签名者自己能做出相应的签名,其他实体是无法做出这样的签名的。这样,签名者从技术上就不能否认自己做过该签名。为了保证签名私钥的安全,一般要求这种密钥只能在防篡改的硬件令牌上产生,并且永远不能离开令牌,以保证签名私钥的安全。

再利用PKI提供的时间戳功能,安全时间戳服务用来证明某个特别事件发生在某个特定的时间,或某段特别数据在某个日期已存在。这样,签名者对自己所做的签名将无法进行

否认。

4. 提供时间戳服务

时间戳也叫做安全时间戳，是一个可信的时间权威，使用一段可以认证的完整数据表示的时间戳。最重要的不是时间本身的精确性，而是相关时间、日期的安全性。支持不可否认服务的一个关键因素就是在PKI中使用安全时间戳，也就是说，时间源是可信的，时间值必须特别安全地传送。

PKI中必须存在用户可信任的权威时间源，权威时间源提供的时间并不需要正确，仅仅需要用户作为一个参照"时间"，以便完成基于PKI的事物处理，如事件A发生在事件B的前面等。一般的PKI系统中都设置一个时钟系统统一PKI的时间。当然也可以使用世界官方时间源所提供的时间，其实现方法是从网络中这个时钟位置获得安全时间。要求实体在需要的时候向这些权威请求在数据上盖上时间戳。一份文档上的时间戳涉及对时间和文档内容哈希值的数字签名。权威的签名提供了数据的真实性和完整性。

虽然安全时间戳是PKI支撑的服务，但它依然可以在不依赖PKI的情况下实现安全时间戳服务。一个PKI体系中是否需要实现时间戳服务，完全依照应用的需求来决定。

5. 保证数据的公正性

PKI中支持的公证服务是指"数据认证"，也就是说，公证人要证明的是数据的有效性和正确性，这种公证取决于数据验证的方式。与公证服务、一般社会公证人提供的服务有所不同，在PKI中被验证的数据是基于杂凑值的数字签名、公钥在数学上的正确性和签名私钥的合法性。

PKI的公证人是一个被其他PKI实体所信任的实体，能够正确地提供公证服务。它主要是通过数字签名机制证明数据的正确性，所以其他实体需要保存公证人的验证公钥的正确备份，以便验证和相信作为公证的签名数据。

通常来说，CA是证书的签发机构，它是PKI的核心。众所周知，构建密码服务系统的核心内容是如何实现密钥的管理。公钥体制涉及一对密钥(即私钥和公钥)，私钥由用户独立掌握，无须在网上传输，而公钥则是公开的，需要在网上传送，故公钥体制的密钥管理主要是针对公钥的管理问题，目前较好的解决方案是数字证书机制。

4.10 认证机构

CA(Certificate Authority)即"认证机构"，是负责签发证书、认证证书、管理已颁发证书的机构，是PKI的核心。CA要制定政策和具体步骤来验证、识别用户的身份，对用户证书进行签名，以确保证书持有者的身份和公钥的拥有权。CA也拥有自己的证书(内含共钥)和私钥，网上用户通过验证CA的签字从而信任CA，任何用户都可以得到CA的证书，用以验证它所签发的证书。CA必须是各行业各部门及公众共同信任的、认可的、权威的、不参与交易的第三方网上身份认证机构。

4.10.1 CA认证机构的功能

1. 证书的颁发

中心接收、验证用户(包括下级认证中心和最终用户)的数字证书的申请，将申请的内容

进行备案,并根据申请的内容确定是否受理该数字证书申请。如果中心接受该数字证书申请,则进一步确定给用户颁发何种类型的证书。新证书用认证中心的私钥签名以后,发送到目录服务器供用户下载和查询。为了保证消息的完整性,返回给用户的所有应答信息都要使用认证中心的签名。

2. 证书的更新

认证中心可以定期更新所有用户的证书,或者根据用户的请求来更新用户的证书。

3. 证书的查询

证书的查询可以分为两类,其一是证书申请的查询,认证中心根据用户的查询请求返回当前用户证书申请的处理过程;其二是用户证书的查询,这类查询由目录服务器来完成,目录服务器根据用户的请求返回适当的证书。

4. 证书的作废

当用户的私钥由于泄密等原因造成用户证书需要申请作废时,用户需要向认证中心提出证书作废的请求,认证中心根据用户的请求确定是否将该证书作废。另外一种证书作废的情况是证书已经过了有效期,认证中心自动将该证书作废。认证中心通过维护证书作废列表(Certificate Revocation List、CRL)来完成上述功能。

5. 证书的归档

证书具有一定的有效期,证书过了有效期之后就将作废,但是不能将作废的证书简单地丢弃,因为有时可能需要验证以前的某个交易过程中产生的数字签名,这时就需要查询作废的证书。基于此类考虑,认证中心还应当具备管理作废证书和作废私钥的功能。

4.10.2 CA 系统的组成

一个典型的 CA 系统包括安全服务器、注册机构 RA、CA 服务器、LDAP 目录服务器和数据库服务器等,如图 4.11 所示。

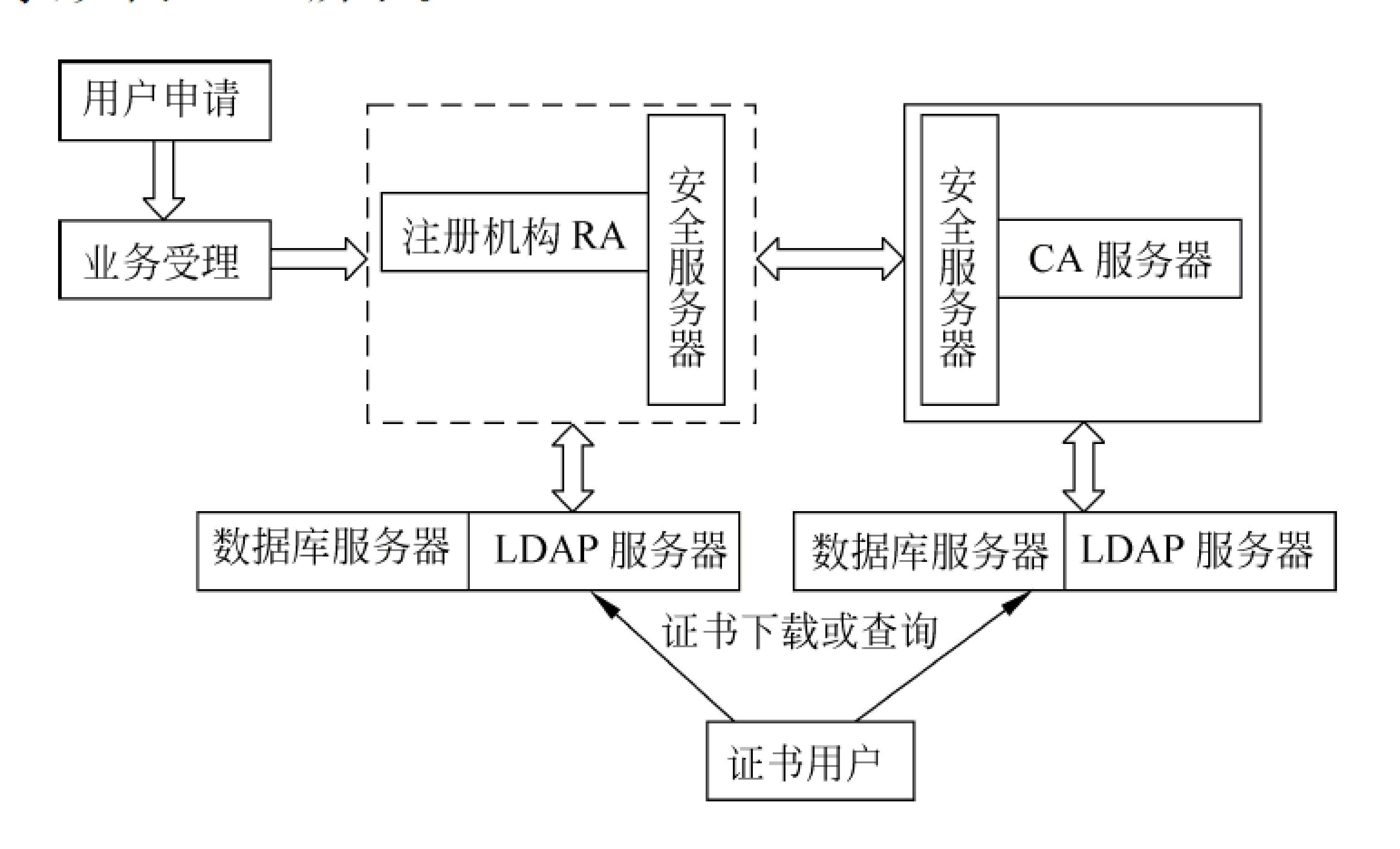


图 4.11 典型 CA 中心示意图

(1) 安全服务器,面向普通用户,用于提供证书申请、浏览、证书撤销列表以及证书下载等安全服务。安全服务器与用户的通信采取安全信道方式(如 SSL 的方式,不需要对用户进行身份认证)。用户首先得到安全服务器的证书(该证书由 CA 颁发),然后用户与服务器之间的所有通信,包括用户填写的申请信息以及浏览器生成的公钥均以安全服务器的密钥

进行加密传输，只有安全服务器利用自己的私钥解密才能得到明文，这样可以防止其他人通过窃听得到明文。从而保证了证书申请和传输过程中的信息安全性。

（2）CA 服务器，是整个证书机构的核心，负责证书的签发。CA 首先产生自身的私钥和公钥（密钥长度至少为 1024 位），然后生成数字证书，并且将数字证书传输给安全服务器。CA 还负责为操作员、安全服务器以及注册机构服务器生成数字证书。安全服务器的数字证书和私钥也需要传输给安全服务器。CA 服务器是整个结构中最为重要的部分，存有 CA 的私钥以及发行证书的脚本文件，出于安全的考虑，应将 CA 服务器与其他服务器隔离，任何通信采用人工干预的方式，确保认证中心的安全。

（3）注册机构 RA，面向登记中心操作员，在 CA 体系结构中起承上启下的作用，一方面向 CA 转发安全服务器传输过来的证书申请请求，另一方面向 LDAP 服务器和安全服务器转发 CA 颁发的数字证书和证书撤销列表。

（4）LDAP 服务器，提供目录浏览服务，负责将注册机构服务器传输过来的用户信息以及数字证书加入到服务器上。这样其他用户通过访问 LDAP 服务器就能够得到其他用户的数字证书。

（5）数据库服务器，是认证机构中的核心部分，用于认证机构中数据（如密钥和用户信息等）、日志和统计信息的存储和管理。实际的数据库系统应采用多种措施，如磁盘阵列、双机备份和多处理器等方式，以维护数据库系统的安全性、稳定性、可伸缩性和高性能。

4.10.3 国内 CA 现状

为促进电子商务在中国的顺利开展，一些行业都已建成了自己的一套 CA 体系，如中国电信 CA 安全认证体系（CTCA）、中国金融认证中心（CFCA）等；还有一些行政区也建立了或正在建立区域性的 CA 体系，如上海电子商务 CA 认证中心（SHECA）、广东省电子商务认证中心（CNCA）、海南省电子商务认证中心（CNCA）、云南省电子商务认证中心（CNCA）等。

1. 中国电信 CA 安全认证系统

中国电信自 1997 年底，开始在长沙进行电子商务试点工作，由长沙电信局负责组织。CTCA 是国内最早的 CA 中心。1999 年 8 月 3 日，中国电信 CA 安全认证系统通过国家密码委员会和信息产业部的联合鉴定，并获得国家信息产品安全认证中心颁发的认证证书，成为首家允许在公网上运营的 CA 安全认证系统。目前，中国电信可以在全国范围内向用户提供 CA 证书服务。

中国电信 CTCA 系统有一套完善的证书发放体系和管理制度。体系采用三级管理结构：全国 CA 安全认证中心（包括全国 CTCA 中心、CTCA 湖南备份中心）、省级 RA 中心以及地市业务受理点，在 2000 年 6 月形成覆盖全国的 CA 证书申请、发放、管理的完整体系。系统为参与电子商务的不同用户提供个人证书、企业证书和服务器证书。同时，中国电信还组织制定了《中国电信电子商务总体技术规范》、《中国电信 CTCA 接口标准》、《网上支付系统的接口标准》、《中国电信电子商务业务管理办法》等，而且中国电信向社会免费公布 CTCA 系统接口标准和 API 软件包，为更多的电子商务应用开发商提供 CTCA 系统的支持与服务。中国电信已经与银行、证券、民航、工商、税务等多个行业联合开发出了网上安全支付系统、电子缴费系统、电子银行系统、电子证券系统、安全电子邮件系统、电子订票系统、网

上购物系统、网上报税等一系列基于中国电信 CTCA 系统的电子商务应用,已经初步建立起中国电信电子商务平台。

2. 中国金融认证中心(CFCA)

中国金融认证中心(CFCA)是由中国人民银行牵头,联合中国工商银行、中国农业银行、中国银行、中国建设银行、交通银行、招商银行、中信实业银行、华夏银行、广东发展银行、深圳发展银行、光大银行、民生银行等十二家商业银行共同建设了中国金融认证中心(China Financial Certificate Authority,CFCA)。中国金融认证中心的项目包括建设 SET CA 和 Non-SET CA 两套系统,工程于 1999 年 8 月 30 日开始实施。SET CA 由 IBM 公司负责承建,Non-SET CA 由 Entrust 公司、SUN 和得达创新联合建设。

Non-SET CA 系统于 2000 年 1 月 19 日发放了第一批试验证书,SET 系统于 2000 年 3 月 30 日试发了第一批证书。于 2000 年 6 月 20 日通过了由国家密码管理委员会和人民银行支付科技司联合主持的密码产品本地化工作的安全性审查。于 2000 年 6 月 29 日开始对社会各界提供证书服务,系统进入运行状态。

中国金融认证中心专门负责为金融业的各种认证需求提供证书服务,包括电子商务、网上银行、网上证券交易、支付系统和管理信息系统等,为参与网上交易的各方提供安全的基础,建立彼此信任的机制。

CFCA 在建设过程中,因为技术上的问题,使得正式发证的时间比以前计划的时间大大推迟。因为在操作上、证书申请的方式上还存在一些问题,因此发放的证书不多。

3. 国富安电子商务安全认证中心

国富安电子商务安全认证中心是中国国际电子商务中心(属外经贸部)下属的专业从事电子商务及信息安全的公司。根据国家"金关工程"网络发展的需要,负责建立、维护、管理、运营中国国际电子商务安全认证中心,并向社会提供数字证书服务。"商业电子信息安全认证系统"已于 1999 年 2 月通过国家科技部和国家密码管理委员会的技术鉴定。

据了解,国富安电子商务安全认证中心的建立借助了国外公司的力量完成的,国富安电子商务安全认证中心自己本身的开发力量一直不强,因此,在它的电子商务证书基础上还没有较多的成功应用,国富安本身在数字证书的基础上也没有完整的应用软件。外经贸部在网上的电子交易很多,但是,其认证系统也没有采用国富安的证书系统。因此其发证量一直比较少。

4. 上海市电子商务安全证书管理中心(SHECA)

上海市电子商务安全证书管理中心由上海市电子商务安全证书管理中心有限公司(简称 SHECA)负责经营管理。上海市电子商务安全证书管理中心属于上海市政府。

SHECA 在上海市政府的大力推广之下,目前发证量相对来说比较多。并且,在 1999 年和 2000 年,SHECA 进行了一些比较成功的推广应用。

比如,东方航空公司网上安全售票系统;上海热线的安全电子邮件服务;基于 SHECA 认证的港澳上证证券之星网上证券交易系统;上海银行卡网络服务中心支付网关;上海网上化工交易中心;基于 SHECA 安全认证的企业名录;并且在上海市政府的介入下,要求上海的各家银行采用 SHECA 颁发的证书。因此 SHECA 在上海得到了比较好的应用。

另外,还有一些其他省级电子商务认证中心,如北京市电子商务认证中心、天津市电子商务认证中心、云南省电子商务认证中心、山东省电子商务认证中心、湖南省电子商务认证

中心、湖北省电子商务认证中心、广东省电子商务认证中心、广西电子商务认证中心、海南省电子商务认证中心、山西省电子商务认证中心、吉林省电子商务认证中心、福建省电子商务认证中心和深圳市电子商务认证中心等。另外，我国还有其他一些省市和企业机关也在着手建立自己的电子商务认证中心，特别是一些大型企业和事业单位，也使用 CA 和证书机制来对企业用户的身份和权限进行认证和管理。

目前，我国的 CA 建设还处于一个起步的阶段，没有完整的统筹和协调，CA 的发展还处于各自为政、独立发展的混乱局面，没有建立一个政策上固定的全国范围的根 CA（如美国的邮政 CA），这对处于权威认证机构的 CA 来说不仅是基础设施的浪费，也对电子商务中的身份认证带来一系列问题，如交叉认证的互不兼容等。相信经过若干年的发展，我国的 CA 建设在积累经验和教训的基础上，一定会形成一个全国性的、完整的和层次性合理的 CA 基础设施，真正为我国的电子商务发展保驾护航。

课后习题

选择题

1. 为了防御网络监听，最常用的方法是（　　）。
A. 采用物理传输（非网络）　　B. 信息加密
C. 无线网　　D. 使用专线传输

2. 下列环节中无法实现信息加密的是（　　）。
A. 链路加密　　B. 上传加密　　C. 节点加密　　D. 端到端加密

3. 基于公开密钥密码体制的信息认证方法采用的算法是（　　）。
A. 素数检测　　B. 非对称算法　　C. RSA 算法　　D. 对称加密算法

4. RSA 算法建立的理论基础是（　　）。
A. DES　　B. 替代相组合
C. 大数分解和素数检测　　D. 哈希函数

5. 防止他人对传输的文件进行破坏需要（　　）。
A. 数字签字及验证　　B. 对文件进行加密
C. 身份认证　　D. 时间戳

6. 下面的机构如果都是认证中心（CA），你认为可以作为资信认证的是（　　）。
A. 国家工商局　　B. 著名企业　　C. 商务部　　D. 人民银行

7. PGP 都随机产生一个（　　）位的 IDEA 会话密钥。
A. 56　　B. 64　　C. 124　　D. 128

8. SHA 的含义是（　　）。
A. 加密密钥　　B. 数字水印　　C. 常用的哈希算法　　D. 消息摘要

9. 保证商业服务不可否认的手段主要是（　　）。
A. 数字水印　　B. 数据加密　　C. 身份认证　　D. 数字签名

10. DES 加密算法所采用的密钥的有效长度为（　　）。
A. 32　　B. 56　　C. 64　　D. 128

11. 数字证书不包含(　　)。

A. 证书的申请日期　　B. 颁发证书的单位

C. 证书拥有者的身份　　D. 证书拥有者姓名

12. 数字签名是解决(　　)问题的方法。

A. 未经授权擅自访问网络　　B. 数据被泄或篡改

C. 冒名发送数据或发送数据后抵赖　　D. 以上三种

13. 在互联网上,不单纯使用对称密钥加密技术对信息进行加密,是因为(　　)。

A. 对称加密技术落后　　B. 加密技术不成熟

C. 密钥难以管理　　D. 人们不了解

14. DES 是一个(　　)加密算法标准。

A. 非对称　　B. 对称　　C. PGP　　D. SSL

15. 利用电子商务进行网上交易,通过(　　)方式保证信息的收发各方都有足够的证据证明操作的不可否认性。

A. 数字信封　　B. 双方信誉　　C. 数字签名　　D. 数字时间戳

填空题

1. 密码学的目的是(　　)、(　　)、(　　)。

2. 身份认证包含(　　)和(　　)两个过程。

3. (　　)及验证是实现信息在公开网络上的安全传输的重要方法,该方法过程实际上是通过(　　)来实现的。

4. PKI/公钥是提供公钥加密和数字签字服务的安全基础平台,目的是管理(　　)和(　　)。

5. 一个典型的 PKI 应用系统包括五个部分:(　　)、(　　)、证书签发子系统、证书发布子系统和目录服务子系统。

6. 密码学根据其研究的范围可分为(　　)和(　　)。

7. (　　)是最为人们所熟悉的古典加密方法,它通常将秘密消息隐藏于其他消息中,使真正的秘密通过一份无伤大雅的消息发送出去。

8. 1977 年,美国的数据加密标准(　　)公布。

9. 密码体制分为(　　)和(　　)。

10. 公钥密码体制的算法中最著名的代表是(　　)系统。

11. (　　),也叫信息标记算法,可以提供数据完整性方面的判断依据。

12. (　　)是一个向个人、计算机或任何其他申请实体颁发证书的可信实体。

简答题

1. 密码学的发展大致可以分为几个阶段? 各阶段的特点是什么?

2. 密码学包含哪些概念? 有什么功能?

3. 简述对称加密算法的基本原理。

4. 简述非对称加密算法的基本原理。

5. 公钥加密系统可提供什么功能?

6. PGP 软件的主要功能有哪些?

7. 简述 PGP 的发信与收信过程。

8. 软件加密的方法有哪些?
9. 用户身份认证的主要目标是什么?基本方式有哪些?
10. 硬件加密特点有哪些?
11. 简述数字签名的原理。
12. 数字签名主要的功能有哪些?
13. 数字证书可以分为几种?各自的用途是什么?
14. 简述一个典型的 PKI 应用系统包括的几个部分。
15. 简述 CA 认证机构的功能。
16. CA 系统由哪几部分组成?

第5章 病毒技术

5.1 病毒的基本概念

5.1.1 计算机病毒的定义

计算机病毒(computer virus)在《中华人民共和国计算机信息系统安全保护条例》中被明确定义,病毒“指编制或者在计算机程序中插入的破坏计算机功能或者破坏数据,影响计算机使用并且能够自我复制的一组计算机指令或者程序代码”。

病毒往往会利用计算机操作系统的弱点进行传播,提高系统的安全性是防病毒的一个重要方面。完美的系统是不存在的,过于强调提高系统的安全性将使系统多数时间用于病毒检查,系统失去了可用性、实用性和易用性;另一方面,信息保密的要求让人们在泄密和抓住病毒之间无法选择。病毒与反病毒将作为一种技术对抗长期存在,两种技术都将随计算机技术的发展而得到长期的发展。

病毒不是来源于突发或偶然的原因。一次突发的停电和偶然的错误,会在计算机的磁盘和内存中产生一些乱码和随机指令,但这些代码是无序和混乱的。而病毒是一种比较完美的、精巧严谨的代码,按照严格的秩序组织起来,与所在的系统网络环境相适应和配合起来的代码。病毒不会通过偶然形成,其代码本身需要有一定的长度,这个基本的长度从概率上来讲是不可能通过随机代码产生的。现在流行的病毒是由人为故意编写的,多数病毒可以找到作者和产地信息,从大量的统计分析来看,病毒作者的主要情况和目的是:一些天才的程序员为了表现自己和证明自己的能力,对上司的不满、好奇、报复、为了祝贺和求爱、为了得到控制口令、为了软件拿不到报酬而预留的陷阱等。当然也有因政治、军事、宗教、民族、专利等方面的需求而专门编写的,其中也包括一些病毒研究机构和黑客的测试病毒。

5.1.2 计算机病毒的特点

计算机病毒具有以下几个特点:

(1) 寄生性。计算机病毒寄生在其他程序之中,当执行这个程序时,病毒就起破坏作用,而在未启动这个程序之前,它是不易被人发觉的。

(2) 传染性。计算机病毒不但本身具有破坏性,更有害的是具有传染性,一旦病毒被复制或产生变种,其速度之快令人难以预防。传染性是病毒的基本特征。在生物界,病毒通过传染从一个生物体扩散到另一个生物体。在适当的条件下,它可得到大量繁殖,并使被感染的生物体表现出病症甚至死亡。同样,计算机病毒也会通过各种渠道从已被感染的计算机扩散到未被感染的计算机,在某些情况下造成被感染的计算机工作失常甚至瘫痪。与生物

病毒不同的是，计算机病毒是一段人为编制的计算机程序代码，这段程序代码一旦进入计算机并得以执行，它就会搜寻其他符合其传染条件的程序或存储介质，确定目标后再将自身代码插入其中，达到自我繁殖的目的。只要一台计算机染毒，如不及时处理，那么病毒会在这台机器上迅速扩散，其中的大量文件(一般是可执行文件)会被感染。而被感染的文件又成了新的传染源，再与其他机器进行数据交换或通过网络接触，病毒会继续进行传染。正常的计算机程序一般是不会将自身的代码强行连接到其他程序之上的。而病毒却能使自身的代码强行传染到一切符合其传染条件的未受到传染的程序之上。计算机病毒可通过各种可能的渠道，如软盘、计算机网络去传染其他计算机。当在一台机器上发现了病毒时，往往曾在这台计算机上用过的软盘已感染上了病毒，而与这台机器相联网的其他计算机也许也被该病毒感染上了。是否具有传染性是判别一个程序是否为计算机病毒的最重要条件。病毒程序通过修改磁盘扇区信息或文件内容并把自身嵌入到其中的方法达到病毒的传染和扩散。被嵌入的程序叫做宿主程序。

(3) 潜伏性。有些病毒像定时炸弹一样，让它什么时间发作是预先设计好的。比如黑色星期五病毒，不到预定时间一点都觉察不出来，等到条件具备的时候一下子就爆炸开来，对系统进行破坏。一个编制精巧的计算机病毒程序，进入系统之后一般不会马上发作，可以在几周或者几个月内甚至几年内隐藏在合法文件中，对其他系统进行传染，而不被人发现，潜伏性越好，其在系统中的存在时间就会越长，病毒的传染范围就会越大。潜伏性的第一种表现是指，病毒程序不用专用检测程序是检查不出来的，因此病毒可以静静地躲在磁盘或磁带里待上几天，甚至几年，一旦时机成熟，得到运行机会，就又要四处繁殖、扩散，继续为害。潜伏性的第二种表现是指，计算机病毒的内部往往有一种触发机制，不满足触发条件时，计算机病毒除了传染外不做什么破坏。触发条件一旦得到满足，有的在屏幕上显示信息、图形或特殊标识，有的则执行破坏系统的操作，如格式化磁盘、删除磁盘文件、对数据文件做加密、封锁键盘以及使系统死锁等。

(4) 隐蔽性。计算机病毒具有很强的隐蔽性，有的可以通过病毒软件检查出来，有的根本就查不出来，有的时隐时现、变化无常，这类病毒处理起来通常很困难。

(5) 破坏性。计算机中毒后，可能会导致正常的程序无法运行，计算机内的文件被删除或受到不同程度的损坏。

(6) 可触发性。因某个事件或数值的出现，诱使病毒实施感染或进行攻击的特性称为可触发性。为了隐蔽自己，病毒必须潜伏，少做动作。如果完全不动，一直潜伏的话，病毒既不能感染也不能进行破坏，便失去了杀伤力。病毒既要隐蔽又要维持杀伤力，它必须具有可触发性。病毒的触发机制就是用来控制感染和破坏动作的频率的。病毒具有预定的触发条件，这些条件可能是时间、日期、文件类型或某些特定数据等。病毒运行时，触发机制检查预定条件是否满足，如果满足，启动感染或破坏动作，使病毒进行感染或攻击；如果不满足，使病毒继续潜伏。

5.1.3 计算机病毒的分类

根据多年对计算机病毒的研究，按照科学的、系统的、严密的方法，根据计算机病毒属性进行如下分类：

(1) 根据病毒存在的媒体进行分类，病毒可以划分为网络病毒、文件病毒、引导型病毒。

① 网络病毒通过计算机网络传播感染网络中的可执行文件。

② 文件病毒感染计算机中的文件(如 COM、EXE、DOC 等)。

③ 引导型病毒感染启动扇区(Boot)和硬盘的系统引导扇区(MBR)。

还有这三种情况的混合型,例如,多型病毒(文件和引导型)感染文件和引导扇区两种目标,这样的病毒通常都具有复杂的算法,它们使用非常规的办法侵入系统,同时使用了加密和变形算法。

(2) 按照计算机病毒传染的方法进行分类,根据病毒传染的方法可分为驻留型病毒和非驻留型病毒。

① 驻留型病毒感染计算机后,把自身的内存驻留部分放在内存(RAM)中,这一部分程序挂接系统调用并合并到操作系统中去,它处于激活状态,一直到关机或重新启动。

② 非驻留型病毒在得到机会激活时并不感染计算机内存,另外一些病毒在内存中留有小部分,但是并不通过这一部分进行传染,这类病毒也被划归为非驻留型病毒。

(3) 根据病毒破坏的能力可划分为以下几种:

① 无害型。除了传染时减少磁盘的可用空间外,对系统没有其他影响。

② 无危险型。这类病毒仅仅是减少内存、显示图像、发出声音及同类音响。

③ 危险型。这类病毒在计算机系统操作中造成严重的错误。

④ 非常危险型。这类病毒删除程序、破坏数据、清除系统内存区和操作系统中重要的信息。

这些病毒对系统造成的危害,并不是本身的算法中存在危险的调用,而是当它们传染时会引起无法预料的和灾难性的破坏。由病毒引起其他程序产生的错误也会破坏文件和扇区,这些病毒也按照它们引起的破坏能力划分。一些现在的无害型病毒也可能会对新版的DOS、Windows 和其他操作系统造成破坏。例如,在早期的病毒中,有一个 Denzuk 病毒在360KB 磁盘上很好地工作,不会造成任何破坏,但是在后来的高密度软盘上却能引起大量的数据丢失。

(4) 根据病毒特有的算法,病毒可以划分为:

① 伴随型病毒。这一类病毒并不改变文件本身,它们根据算法产生 EXE 文件的伴随体,具有同样的名字和不同的扩展名(COM),例如,XCOPY. EXE 的伴随体是 XCOPY. COM。病毒把自身写入 COM 文件并不改变 EXE 文件,当 DOS 加载文件时,伴随体优先被执行到,再由伴随体加载执行原来的 EXE 文件。

② “蠕虫”型病毒。通过计算机网络传播,不改变文件和资料信息,利用网络从一台机器的内存传播到其他机器的内存,计算网络地址,将自身的病毒通过网络发送。有时它们在系统存在,一般除了内存不占用其他资源。

③ 寄生型病毒。除了伴随型和“蠕虫”型,其他病毒均可称为寄生型病毒,它们依附在系统的引导扇区或文件中,通过系统的功能进行传播。

④ 诡秘型病毒。它们一般不直接修改 DOS 中断和扇区数据,而是通过设备技术和文件缓冲区等 DOS 内部修改,不易看到资源,使用比较高级的技术。利用 DOS 空闲的数据区进行工作。

⑤ 变型病毒(又称幽灵病毒)。这一类病毒使用一个复杂的算法,使自己每传播一份都具有不同的内容和长度。它们一般是由一段混有无关指令的解码算法和被变化过的病毒体

组成。

5.1.4 计算机病毒的发展史

在病毒的发展史上，病毒的出现是有规律的，一般情况下一种新的病毒技术出现后，病毒迅速发展，接着反病毒技术的发展会抑制其流传。操作系统升级后，病毒也会调整为新的方式，产生新的病毒技术。它可划分为：

（1）DOS 引导阶段。1987 年，计算机病毒主要是引导型病毒，具有代表性的是“小球”和“石头”病毒。当时的计算机硬件较少，功能简单，一般需要通过软盘启动后使用。引导型病毒利用软盘的启动原理工作，它们修改系统启动扇区，在计算机启动时首先取得控制权，减少系统内存，修改磁盘读写中断，影响系统工作效率，在系统存取磁盘时进行传播；1989 年，引导型病毒发展为可以感染硬盘，典型的代表有“石头 2”。

（2）DOS 可执行阶段。1989 年，可执行文件型病毒出现，它们利用 DOS 系统加载执行文件的机制工作，代表为“耶路撒冷”、“星期天”病毒，病毒代码在系统执行文件时取得控制权，修改 DOS 中断，在系统调用时进行传染，并将自己附加在可执行文件中，使文件长度增加。1990 年，发展为复合型病毒，可感染 COM 和 EXE 文件。

（3）伴随、批次型阶段。1992 年，伴随型病毒出现，它们利用 DOS 加载文件的优先顺序进行工作，具有代表性的是“金蝉”病毒，它感染 EXE 文件时生成一个和 EXE 同名但扩展名为 COM 的伴随体；它感染文件时，修改原来的 COM 文件为同名的 EXE 文件，再产生一个原名的伴随体，文件扩展名为 COM，这样，在 DOS 加载文件时，病毒就取得控制权。这类病毒的特点是不改变原来的文件内容、日期及属性，解除病毒时只要将其伴随体删除即可。在非 DOS 操作系统中，一些伴随型病毒利用操作系统的描述语言进行工作，典型代表是“海盗旗”病毒，它在得到执行时，询问用户名称和口令，然后返回一个出错信息，将自身删除。批次型病毒是工作在 DOS 下的和“海盗旗”病毒类似的一类病毒。

（4）幽灵、多形阶段。1994 年，随着汇编语言的发展，实现同一功能可以用不同的方式进行完成，这些方式的组合使一段看似随机的代码产生相同的运算结果。幽灵病毒就是利用这个特点，每感染一次就产生不同的代码。例如“一半”病毒就是产生一段有上亿种可能的解码运算程序，病毒体被隐藏在解码前的数据中，查解这类病毒就必须能对这段数据进行解码，加大了查毒的难度。多形型病毒是一种综合性病毒，它既能感染引导区又能感染程序区，多数具有解码算法，一种病毒往往要两段以上的子程序方能解除。

（5）生成器、变体机阶段。1995 年，在汇编语言中，一些数据的运算放在不同的通用寄存器中，可运算出同样的结果，随机插入一些空操作和无关指令，也不影响运算的结果，这样，一段解码算法就可以由生成器生成，当生成器的生成结果为病毒时，就产生了这种复杂的“病毒生成器”，而变体机就是增加解码复杂程度的指令生成机制。这一阶段的典型代表是“病毒制造机”VCL，它可以在瞬间制造出成千上万种不同的病毒，查解时就不能使用传统的特征识别法，需要在宏观上分析指令，解码后查解病毒。

（6）网络、蠕虫阶段。1995 年，随着网络的普及，病毒开始利用网络进行传播，它们只是以上几代病毒的改进。在非 DOS 操作系统中，“蠕虫”是典型的代表，它不占用除内存以外的任何资源，不修改磁盘文件，利用网络功能搜索网络地址，将自身向下一地址进行传播，有时也在网络服务器和启动文件中存在。

（7）视窗阶段。1996年，随着Windows的日益普及，利用Windows进行工作的病毒开始发展，它们修改(NE、PE)文件格式的文件，典型的代表是DS.3873，这类病毒的机制更为复杂，它们利用保护模式和API调用接口工作，解除方法也比较复杂。

（8）宏病毒阶段。1996年，随着Windows Word功能的增强，使用Word宏语言也可以编制病毒，这种病毒使用类Basic语言、编写容易、感染Word文档等文件，在Excel和AmiPro出现的相同工作机制的病毒也归为此类，由于Word文档格式没有公开，这类病毒查解比较困难。

（9）互联网阶段。1997年，随着因特网的发展，各种病毒也开始利用因特网进行传播，一些携带病毒的数据包和邮件越来越多，如果不小心打开了这些邮件，机器就有可能中毒。1997年，随着Java的普及，利用Java语言进行传播和资料获取的病毒开始出现，典型的代表是JavaSnake病毒，还有一些利用邮件服务器进行传播和破坏的病毒，例如Mail-Bomb病毒，它会严重影响因特网的效率。

5.1.5 其他破坏行为

计算机病毒的破坏行为体现了病毒的杀伤能力。病毒破坏行为的激烈程度取决于病毒作者的主观愿望和他所具有的技术能量。数以万计不断发展扩张的病毒，其破坏行为千奇百怪，不可能穷举其破坏行为，而且难以做全面的描述，根据现有的病毒资料可以把病毒的破坏目标和攻击部位归纳如下。

（1）攻击系统数据区，攻击部位包括硬盘主引导扇区、Boot扇区、FAT表、文件目录等。一般来说，攻击系统数据区的病毒是恶性病毒，受损的数据不易恢复。

（2）攻击文件，病毒对文件的攻击方式很多，可列举如下：删除、改名、替换内容、丢失部分程序代码、内容颠倒、写入时间空白、变碎片、假冒文件、丢失文件簇、丢失数据文件等。

（3）攻击内存，内存是计算机的重要资源，也是病毒攻击的主要目标之一，病毒额外地占用和消耗系统的内存资源，可以导致一些较大的程序难以运行。病毒攻击内存的方式如下：占用大量内存、改变内存总量、禁止分配内存、蚕食内存等。

（4）干扰系统运行，此类型病毒会干扰系统的正常运行，以此作为自己的破坏行为，此类行为也是花样繁多，可以列举下述诸方式：不执行命令、干扰内部命令的执行、虚假报警、使文件打不开、使内部栈溢出、占用特殊数据区、时钟倒转、重启动、死机、强制游戏、扰乱串行口、并行口等。

（5）速度下降，病毒激活时，其内部的时间延迟程序启动，在时钟中纳入了时间的循环计数，迫使计算机空转，计算机速度明显下降。攻击磁盘，攻击磁盘数据、不写盘、写操作变读操作、写盘时丢字节等。

（6）扰乱屏幕显示，例如字符跌落、环绕、倒置、显示前一屏、光标下跌、滚屏、抖动、乱写、吃字符等。

（7）键盘病毒，干扰键盘操作，已发现有下述方式：响铃、封锁键盘、换字、抹掉缓存区字符、重复、输入紊乱等。

（8）喇叭病毒，许多病毒运行时，会使计算机的喇叭发出响声。有的病毒作者通过喇叭发出种种声音，有的病毒作者让病毒演奏旋律优美的世界名曲，在高雅的曲调中去杀戮人们的信息财富，已发现的喇叭发声有以下方式：演奏曲子、警笛声、炸弹噪声、鸣叫、咔咔声、滴

答声等。

(9) 攻击 CMOS,在机器的 CMOS 区中,保存着系统的重要数据,例如系统时钟、磁盘类型、内存容量等。有的病毒激活时,能够对 CMOS 区进行写入动作,破坏系统 CMOS 中的数据。

5.1.6 计算机病毒的危害性

计算机资源的损失和破坏,不但会造成资源和财富的巨大浪费,而且有可能造成社会性的灾难,随着信息化社会的发展,计算机病毒的威胁日益严重,反病毒的任务也更加艰巨了。1988 年 11 月 2 日下午 5 时 1 分 59 秒,美国康奈尔大学的计算机科学系研究生,23 岁的莫里斯(Morris)将其编写的蠕虫程序输入计算机网络,致使这个拥有数万台计算机的网络被堵塞。这件事就像是计算机界的一次大地震,引起了巨大反响,震惊全世界,引起了人们对计算机病毒的恐慌,也使更多的计算机专家重视和致力于计算机病毒的研究。1988 年下半年,我国在统计局系统首次发现了"小球"病毒,它对统计系统影响极大,此后由计算机病毒发作而引起的"病毒事件"接连不断,后来发现的 CIH、美丽莎、冲击波、震荡波等病毒更是给社会造成了很大损失。

2000 年 5 月爆发的"爱虫"病毒及其以后出现的 50 来个变种病毒让计算机信息界付出了很大代价,共感染了 4000 多万台计算机,造成大约 87 亿美元的经济损失。1999 年共出现了两种代价超过 10 亿美元的"昂贵"病毒——"爱丽莎"病毒和"探测者"病毒,它们分别造成了 12 亿和 10 亿美元的经济损失。2001 年 7 月"红色代码"病毒爆发后,在短短 9 个小时内感染了超过 25 万台计算机系统,引起了各国政府官员和计算机安全人员的高度恐慌。

2004 年严重肆虐全球个人计算机的知名病毒"杀手"(Sasser)和"天网"(Netsky),均导致高达百万部计算机中毒,财务损失和修复成本分别高达 35 亿美元、27.5 亿美元。"末日"(MyDoom)对微软和 SCO Group 公司网站发动攻击,蔓延迅速,估计财务损失高达 52.5 亿美元,相当可观。

计算机病毒不仅对计算机产生影响,而且对人也会产生一定影响。当然计算机病毒是不会与人交叉感染的,那么它是怎样对人产生影响的呢?其实很简单,它是通过控制屏幕的输出来对人的心理进行影响。有些按破坏能力分类归为"无害"的病毒,虽然不会损坏数据,但在发作时并不只是播放一段音乐这样简单。有些病毒会进行反动宣传,有些病毒会显示一些对人身心健康不利的文字或图像。在 2000 年底,人们发现了一个通过电子邮件传播的病毒——"女鬼"病毒。当你打开感染了"女鬼"病毒的邮件的附件时,病毒发作,在屏幕上显示一个美食家杀害妻子的恐怖故事。之后,一切恢复正常。一般人会以为这个病毒的发作只是这样而已。但是,5 分钟后,突然屏幕变黑,一个恐怖的女尸的图像就会显示出来,让没有丝毫心理准备的人吓一跳。据报道,有人因此突发心脏病身亡。所以,计算机病毒的这个危害也是不可小视的。

5.2 网络病毒

网络病毒通过计算机网络传播感染网络中的可执行文件(如 COM、EXE、DOC 等),网络病毒主要进行游戏等账号的盗取工作,远程操控,或把受控者的计算机当作肉鸡使用。

具有开放性的互联网成为计算机病毒广泛传播的有利环境，而互联网本身的安全漏洞为培育新一代病毒提供了绝佳的条件。人们为了让网页更加精彩漂亮、功能更加强大而开发出 Active X 技术和 Java 技术，然而病毒程序的制造者也利用同样的渠道，把病毒程序由网络渗透到个人计算机中。这就是近几年崛起的第二代病毒，即所谓的“网络病毒”。可以说：“网络：病毒的天堂”。

2000 年出现的“罗密欧与朱丽叶”病毒是一个典型的网络病毒，它改写了病毒的历史。在当时，人们还以为病毒技术的发展速度不会太快，然而“罗密欧与朱丽叶”病毒彻底击碎了人们的侥幸心理。“罗密欧与朱丽叶”病毒具有邮件病毒的所有特性，但它不再藏身于电子邮件的附件中，而是直接存在于邮件正文中，一旦计算机用户用 Outlook 打开邮件进行阅读，病毒就会立即发作，并将复制出的新病毒通过邮件发送给其他人，计算机用户几乎无法躲避。

网络病毒的出现似乎拓展了病毒制造者们的思路，在随后的时间里，千奇百怪的网络病毒孕育而生。这些病毒具有更强的繁殖能力和破坏能力，它们不再局限于电子邮件之中，而是直接钻入 Web 服务器的网页代码中，当计算机用户浏览了带有病毒的网页之后，系统就会被感染，随即崩溃。当然，这些病毒也不会放过自己寄生的服务器，在适当的时候病毒会与服务器系统同归于尽。

公安部国家计算机病毒应急处理中心、计算机病毒防治产品检验中心联合发布了《2008 年我国信息网络安全状况暨计算机病毒疫情调查报告》。调查结果显示，我国信息网络安全事件发生比例继前 3 年连续增长后，2008 年略有下降，信息网络安全事件发生比例为 62.7%，比 2007 年下降了 3%；计算机病毒感染率也出现下降，为 85.5%，比 2007 年减少了 6%。奥运期间，全国互联网安全状况基本平稳，未出现重大网络安全事件。

近年来病毒功能越来越强大，不仅拥有蠕虫病毒的传播速度和破坏能力，还具有木马的控制计算机和盗窃重要信息的功能。2000 年以来，病毒制作者为了获得经济利益，纷纷开始制作各类木马，一时间网上木马横行。

2006 年“熊猫烧香”这一复合型病毒的出现，改变了病毒制作者的想法。利用蠕虫的传播能力和多种传播渠道，可以更快更多地帮助木马传播，从而攫取更大的非法经济效益。因此，“熊猫烧香”病毒在几个月的时间里感染了大量机器，给被感染的用户带来重大损失。

据悉，通过对 2007 年十大病毒的统计，结果显示 2006 年十大病毒的一半还在 2007 年十大病毒的列表中，并且“木马代理”继 2006 年之后，再度成为 2007 年的最流行病毒。2007 年十大病毒排行榜分别为：木马代理、网游大盗、艾妮、熊猫烧香、梅勒斯、德芙、灰鸽子、Small 及其变种、QQ 木马、传奇木马。2008 年十大病毒排行榜分别为：网游大盗、AutoRun、JS. Agent、Delf(德芙)、AV 终结者、灰鸽子、Small 及其变种、JS. RealPlr、JS. Psyme、HTML. Iframe。

自 2001 年开始病毒疫情调查工作以来，没有出现过同一种病毒连续两年成为十大病毒榜首的情况，而 2006 年到 2008 年的数据中木马代理、网游大盗连续出现，这也表明木马具有强大的生存能力。十大病毒中与盗取密码有关的病毒还有“网游大盗”、“艾妮”、“熊猫烧香”、“梅勒斯”、“QQ 木马”和“传奇木马”、“灰鸽子”，它们都具有窃取用户的游戏账号和密码的功能。

5.2.1 木马病毒的概念

特洛伊木马(简称木马),英文叫做 Trojan horse,其名称取自希腊神话的特洛伊木马记。故事说的是希腊人围攻特洛伊城十年后仍不能得手,于是阿迦门农受雅典娜的启发:把士兵藏匿于巨大无比的木马中,然后佯作退兵。当特洛伊人将木马作为战利品拖入城内时,高大的木马正好卡在城门间,进退两难。夜晚木马内的士兵爬出来,与城外的部队里应外合而攻下了特洛伊城。计算机世界的特洛伊木马是指隐藏在正常程序中的一段具有特殊功能的恶意代码,是具备破坏和删除文件、发送密码、记录键盘和 DoS 攻击等特殊功能的后门程序。它是一种基于远程控制的黑客工具,具有隐蔽性和非授权性的特点。

所谓隐蔽性是指木马的设计者为了防止木马被发现,会采用多种手段隐藏木马,这样服务端即使发现感染了木马,由于不能确定其具体位置,往往只能望"马"兴叹。

所谓非授权性是指一旦控制端与服务端连接后,控制端将享有服务端的大部分操作权限,包括修改文件,修改注册表,控制鼠标、键盘等,而这些权力并不是服务端赋予的,而是通过木马程序窃取的。

木马和病毒都是一种人为的程序,都属于计算机病毒,为什么木马要单独提出来说?大家都知道以前的计算机病毒的作用,其实完全就是为了搞破坏,破坏计算机里的资料数据,除了破坏之外有些病毒制造者为了达到某些目的而进行的威慑或敲诈勒索,或为了炫耀自己的技术。木马不一样,木马的作用是赤裸裸地偷偷监视别人和盗窃别人密码、数据等。如盗窃管理员密码、子网密码搞破坏,或者好玩,偷窃上网密码用于他用,游戏账号、股票账号、网上银行账户等。达到偷窥别人隐私和得到经济利益的目的。所以木马比早期的计算机病毒更加有害。更能够直接达到使用者的目的,导致许多别有用心的程序开发者大量地编写这类带有偷窃和监视别人计算机的侵入性程序,这就是目前网上大量木马泛滥成灾的原因。鉴于木马的这些巨大危害性和它与早期病毒的作用性质不一样,因此木马虽然属于病毒中的一类,但是要单独地从病毒类型中间剥离出来,特别地称之为"木马"程序。

木马的发展可以分为以下几个阶段。

1. 第一代木马:伪装型病毒

这种病毒通过伪装成一个合法性程序诱骗用户上当。世界上第一个计算机木马是出现在 1986 年的 PC-Write 木马。它伪装成共享软件 PC-Write 的 2.72 版本(事实上,编写 PC-Write 的 Quicksoft 公司从未发行过 2.72 版本),一旦用户信以为真运行该木马程序,那么他的下场就是硬盘被格式化。有人用 BASIC 作了一个登录界面木马程序,当用户把他的用户 ID、密码输入一个和正常的登录界面一模一样的伪登录界面后,木马程序一面保存用户的 ID 和密码,一面提示用户密码错误让用户重新输入,当用户第二次登录时,就已成了木马的牺牲品。此时的第一代木马还不具备传染特征。

2. 第二代木马:AIDS 型木马

继 PC-Write 之后,1989 年出现了 AIDS 木马。由于当时很少有人使用电子邮件,所以 AIDS 的作者就利用现实生活中的邮件进行散播:给其他人寄去一封封含有木马程序软盘的邮件。之所以叫这个名称是因为软盘中包含有 AIDS 和 HIV 疾病的药品、价格以及预防措施等相关信息。软盘中的木马程序在运行后,虽然不会破坏数据,但是它将硬盘加密锁死,然后提示受感染用户花钱消灾。可以说第二代木马已具备了传播特征(尽管通过传统的

邮递方式)。

3. 第三代木马：网络传播性木马

随着 Internet 的普及，这一代木马兼备伪装和传播两种特征并结合 TCP/IP 网络技术四处泛滥。同时它还添加了新的特征“后门”功能。所谓后门就是一种可以为计算机系统秘密开启访问入口的程序。一旦被安装，这些程序就能够使攻击者绕过安全程序进入系统。该功能的目的就是收集系统中的重要信息，例如，财务报告、口令及信用卡号。此外，攻击者还可以利用后门控制系统，使之成为攻击其他计算机的帮凶。由于后门是隐藏在系统背后运行的，因此很难被检测到。它们不像病毒和蠕虫那样通过消耗内存而引起注意。图 5.1 为 QQ 软件中木马病毒时的现象。

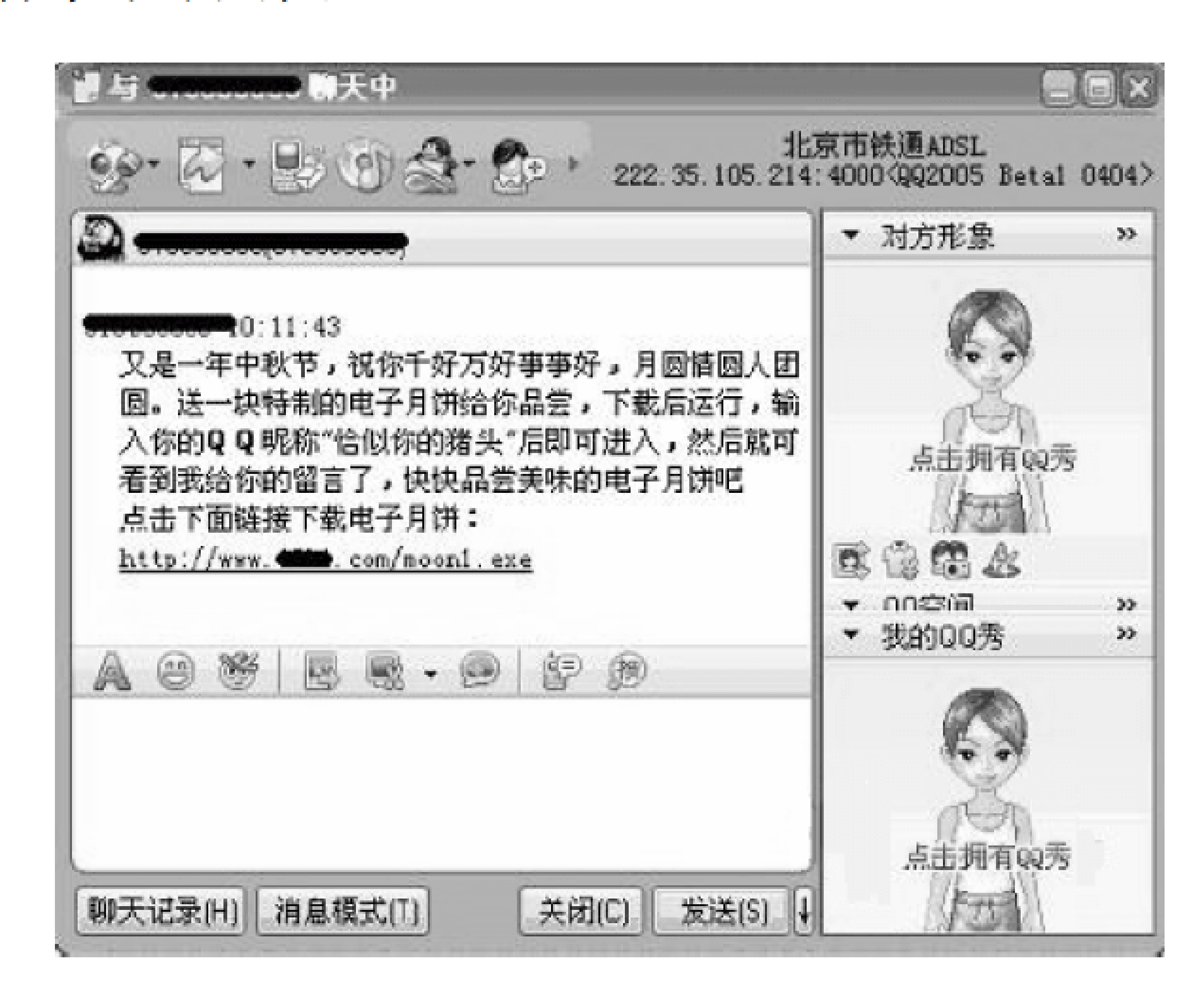


图 5.1　QQ 软件中木马病毒时的现象

添加了击键记录功能。从名称上就可以知道，该功能主要是记录用户所有的击键内容然后形成击键记录的日志文件发送给恶意用户。恶意用户可以从中找到用户名、口令以及信用卡号等用户信息。这一代木马比较有名的有国外的 BO2000 和国内的冰河木马。它们有如下共同特点：基于网络的客户端/服务器应用程序，具有搜集信息、执行系统命令、重新设置机器、重新定向等功能。当木马程序攻击得手后，计算机就完全成为黑客控制的傀儡主机，黑客成了超级用户，用户的所有计算机操作不但没有任何秘密而言，而且黑客可以远程控制傀儡主机对别的主机发动攻击，这时候被俘获的傀儡主机成了黑客进行进一步攻击的挡箭牌和跳板。

虽然木马程序手段越来越隐蔽，但是苍蝇不叮无缝的蛋，只要加强个人安全防范意识，还是可以大大降低“中招”的几率。对此有如下建议：安装个人防病毒软件、个人防火墙软件；及时安装系统补丁；对不明来历的电子邮件和插件不予理睬；经常去安全网站转一转，以便及时了解一些新木马的底细，做到知己知彼，百战不殆。

5.2.2　木马病毒案例

1. “顶狐”木马病毒网上银行盗窃案

2007 年 12 月 16 日，“3.5”特大网上银行盗窃案的 8 名主要犯罪嫌疑人全部落入法网。8 名疑犯在网上以虚拟身份联系，纠集成伙，虽不明彼此身份，却配合密切，分工明确，有人

制作木马病毒、有人负责收集信息、有人提现、有人收赃，在不到一年时间里窃得人民币300余万元。其中，徐伟冲提供信息，金星通过网上购买游戏点卡，转手倒卖给湖南长沙的“宝宝”。因信息太多，忙不过来，金星又在网上将信息倒卖给“小胖”、徐小兵，“小胖”、徐小兵再转卖他人提现。陆瑛娜则不停地在网上购游戏点卡，她到外地制作了两张假身份证，在数家银行开了账户，忙着到苏州、昆山、常州等周边地区银行去取赃款……

2008年4月11日，无锡市滨湖区法院对一起公安部挂牌督办的重大网络犯罪案件作出了一审判决，被告人金星、徐伟冲、陆瑛娜、龚永强、徐小兵、方少宏等因构成信用卡诈骗罪和盗窃罪，分别被判处十四年至三年不等的有期徒刑。

2. 利用DNS劫持攻击大型网站恶性攻击事件

2007年11月3日，部分用户在访问腾讯迷你首页网站(http://minisite.qq.com/)时，会被恶意代码感染，系统会自动从恶意网站上下载并运行恶意程序。由于该站点为QQ软件启动时默认自动弹出，具有极高的访问量，攻击者采用的攻击方法是劫持DNS解析过程，篡改腾讯迷你首页的DNS记录。

非法劫持腾讯“迷你网”主页域名传播17种32个计算机木马病毒，使全国数百万网民在访问“迷你网”主页，玩传奇、魔兽等网络游戏时，游戏账号和密码被秘密发送到木马程序设置的远程接收服务器上，该团伙迅速盗取账号和密码，在网上销赃套现，销赃所得按“贡献”大小分成。不到两个月时间，涉案人员盗窃数十万网上用户的游戏账号和密码，非法获利40余万元。腾讯“迷你网”因停止服务，造成直接损失20余万元。

2007年11月19日，无锡市公安局网警支队接报：当月5日至19日期间，全国部分地区的互联网用户在访问深圳市腾讯计算机系统有限公司迷你网主页时，被错误指向到位于无锡市的病毒服务器，造成上百万网民的计算机受病毒感染，腾讯公司被迫停止网站服务，造成重大经济损失。警方立即开展侦查，于同年12月，分别在四川成都、江苏张家港、黑龙江东宁等地抓获6名犯罪嫌疑人。江苏省公安厅信息网络安全监察部门在犯罪嫌疑人使用的计算机硬盘中发现了用于攻击网站的破坏性程序。经审查，2007年9月底至11月中旬，这一团伙在成都市使用编译好的劫持程序对上海、重庆、扬州等10余个城市共计27台域名服务器实施攻击劫持，借机盗取网络游戏账号。

法院审理认为，6名被告违反国家规定，对计算机信息系统功能进行干扰，造成计算机信息系统不能正常运行，后果严重，均已构成破坏计算机信息系统罪。马志松等6名被告分别被江苏无锡滨湖区法院一审判处四年至一年不等有期徒刑。

5.2.3 蠕虫病毒的概念

蠕虫病毒是一种常见的计算机病毒。它的传染机理是利用网络进行复制和传播，传染途径是通过网络、电子邮件以及优盘、移动硬盘等移动存储设备。比如2006年底的“熊猫烧香”病毒就是蠕虫病毒的一种。蠕虫程序主要利用系统漏洞进行传播。它通过网络、电子邮件和其他传播方式，像生物蠕虫一样从一台计算机传染到另一台计算机。因为蠕虫使用多种方式进行传播，所以蠕虫程序的传播速度是非常大的。

蠕虫侵入一台计算机后，首先获取其他计算机的IP地址，然后将自身副本发送给这些计算机。蠕虫病毒也使用存储在染毒计算机上的邮件客户端地址簿里的地址来传播程序。虽然有的蠕虫程序也在被感染的计算机中生成文件，但一般情况下，蠕虫程序只占用内存资

源而不占用其他资源。

蠕虫也是一种病毒,因此具有病毒的共同特征。一般的病毒是需要寄生的,它可以通过自己指令的执行,将自己的指令代码写到其他程序的体内,而被感染的文件被称为“宿主”。例如,Windows 下可执行文件的格式为 PE 格式,需要感染 PE 文件时,首先在宿主程序中,然后建立一个新段,将病毒代码写到新段中,修改程序入口点等,这样,宿主程序执行的时候,就可以先执行病毒程序,病毒程序运行完之后,再把控制权交给宿主原来的程序指令。可见,病毒主要是感染文件,当然也还有像 DIRII 这种链接型病毒,还有引导区病毒。引导区病毒是感染磁盘的引导区,如果是软盘、U 盘(闪存盘)、移动硬盘等被感染,其受感染的盘在其他机器上使用后,同样也会感染其他机器,所以传播方式也可以是移动存储设备。

蠕虫一般不采取利用 PE 格式插入文件的方法,而是复制自身在互联网环境下进行传播,病毒的传染能力主要是针对计算机内的文件系统而言,而蠕虫病毒的传染目标是互联网内的所有计算机。局域网条件下的共享文件夹、电子邮件、网络中的恶意网页、大量存在着漏洞的服务器等都成为蠕虫传播的良好途径。网络的发展也使得蠕虫病毒可以在几个小时内蔓延全球,而且蠕虫的主动攻击性和突然爆发性将使得人们手足无措。

蠕虫病毒由两部分组成：一个主程序和一个引导程序。主程序一旦在机器上建立就会去收集与当前机器联网的其他机器的信息。它能通过读取公共配置文件并运行显示当前网上联机状态信息的系统实用程序而做到这一点。随后,它尝试利用前面所描述的那些缺陷在这些远程机器上建立其引导程序。

蠕虫病毒程序常驻于一台或多台机器中,并有自动重新定位的能力。如果它检测到网络中的某台机器未被占用,它就把自身的一个复制(一个程序段)发送给那台机器。每个程序段都能把自身的复制重新定位于另一台机器中,并且能识别它占用的那台机器。

蠕虫的行为特征主要包括：主动攻击、行踪隐蔽、利用系统和网络应用服务漏洞、造成网络拥塞、降低系统性能、产生安全隐患、反复性、破坏性等。

1. 蠕虫技术发展的几个趋势

(1) 与病毒技术的结合,一些病毒编写者很早就提出过这样的思路,现在已经变成了现实。越来越多的蠕虫开始结合病毒技术,在攻击计算机系统之后,继续攻击文件系统,从而导致传播机制的多样化。

(2) 动态功能升级技术,提出动态调整蠕虫程序的思路顺理成章,这样的蠕虫可以升级上文提到的功能模型中的除控制模块外的所有功能模块,从而获得更强的生存能力和攻击能力。

(3) 通信技术,蠕虫之间、编写者与蠕虫之间传递信息和指令的功能将成为未来蠕虫编写的重点技术。

(4) 隐身技术,操作系统内核一级的黑客攻防技术将会进一步纳入到蠕虫的功能中来隐藏蠕虫的踪迹。

(5) 巨型蠕虫,蠕虫程序包含多操作系统的运行程序版本,包含丰富的漏洞库,从而具有更强大的传染能力。

(6) 分布式蠕虫,数据部分同运行代码分布在不同的计算机之间,运行代码在攻击时,从数据存放地获取攻击信息。同时,攻击代码利用一些算法在多台计算机上寻找、复制数据

的存放地。不同功能模块分布在不同的计算机之间，协调工作，产生更强的隐蔽性和攻击能力。

2. 蠕虫发作的几种情况

(1) 利用操作系统和应用程序的漏洞主动进行攻击，此类病毒主要是“红色代码”、“尼姆亚”、“求职信”等。由于IE浏览器的漏洞，使得感染了“尼姆亚”病毒的邮件在不去手工打开附件的情况下病毒就能激活，而此前即便是很多防病毒专家也一直认为，带有病毒附件的邮件，只要不去打开附件，病毒不会有危害。“红色代码”利用微软IIS服务器软件的漏洞(idq.dll远程缓存区溢出)来传播，SQL蠕虫王病毒则利用微软的数据库系统的一个漏洞进行大肆攻击。

(2) 传播方式多样，如“尼姆亚”和“求职信”病毒，可利用的传播途径包括文件、电子邮件、Web服务器、网络共享等。

(3) 新的制作技术，与传统的病毒不同的是，许多新病毒是利用当前最新的编程语言与编程技术实现的，易于修改以产生新的变种，从而逃避反病毒软件的搜索。另外，新病毒利用Java、ActiveX、VB Script等技术，可以潜伏在HTML页面里，在上网浏览时触发。

(4) 与黑客技术相结合，潜在的威胁和损失更大，以红色代码为例，感染后的机器的Web目录的\scripts下将生成一个root.exe，可以远程执行任何命令，从而使黑客能够再次进入。

蠕虫和普通病毒不同的一个特征是蠕虫病毒往往能够利用缺陷，即软件上的缺陷和人为的缺陷。软件上的缺陷，如远程溢出、微软IE和Outlook的自动执行漏洞等，需要软件厂商和用户共同配合，不断地升级软件。而人为的缺陷，主要指的是计算机用户的疏忽。这就是所谓的社会工程学，当收到一封带着病毒的求职信邮件时候，大多数人都会抱着好奇的心理去点击。对于企业用户来说，威胁主要集中在服务器和大型应用软件的安全上，而对个人用户而言，主要是防范第二种缺陷。

3. 个人用户对蠕虫病毒的防范措施

通过上述的分析和介绍，我们可以知道，病毒并不是非常可怕的，网络蠕虫病毒对个人用户的攻击主要还是通过社会工程学，而不是利用系统漏洞，所以防范此类病毒需要注意以下几点：

(1) 选购合适的杀毒软件，网络蠕虫病毒的发展已经使传统的杀毒软件的“文件级实时监控系统”落伍，杀毒软件必须向内存实时监控和邮件实时监控发展。另外，面对防不胜防的网页病毒，也使得用户对杀毒软件的要求越来越高。

(2) 经常升级病毒库，杀毒软件对病毒的查杀是以病毒的特征码为依据的，而病毒每天都层出不穷，尤其是在网络时代，蠕虫病毒的传播速度快、变种多，所以必须随时更新病毒库，以便能够查杀最新的病毒。

(3) 提高防杀毒意识。不要轻易去点击陌生的站点，有可能里面就含有恶意代码。当运行IE时，选择“工具”→“Internet选项”→“安全”→“Internet区域的安全级别”命令，把安全级别由“中”改为“高”。因为这一类网页主要是含有恶意代码的ActiveX或Applet、JavaScript的网页文件，所以在IE设置中将ActiveX插件和控件、Java脚本等全部禁止，就可以大大减少被网页恶意代码感染的几率。具体操作是在IE窗口中单击“工具”→“Internet选项”→“安全”→“Internet自定义级别”按钮，如图5.2所示。就会弹出“安全设

置”对话框，把其中所有 ActiveX 插件和控件以及与 Java 相关的全部选项选择“禁用”。但是，这样做在以后的网页浏览过程中有可能会使一些正常应用 ActiveX 的网站无法浏览。

（4）不随意查看陌生邮件，尤其是带有附件的邮件。由于有的病毒邮件能够利用 IE 和 Outlook 的漏洞自动执行，所以计算机用户需要升级 IE 和 Outlook 程序，以及其他常用的应用程序。

（5）打好相应的系统补丁，可以应用瑞星杀毒软件的“漏洞扫描”或 360 安全卫士等工具，这些款工具可以引导用户打好补丁并进行相应的安全设置，彻底杜绝病毒的感染。

（6）警惕聊天软件发来的信息，从 2004 年起，MSN 、QQ 等聊天软件开始成为蠕虫病毒传播的途径之一。“性感烤鸡”病毒就通过 MSN 软件传播，在很短时间内席卷全球，一度造成中国内地部分网络运行异常。对于普通用户来讲，防范聊天蠕虫的主要措施之一，就是提高安全防范意识，对于通过聊天软件发送的任何文件和信息，都要经过好友确认后再运行，不要随意点击聊天软件发送的网络链接。

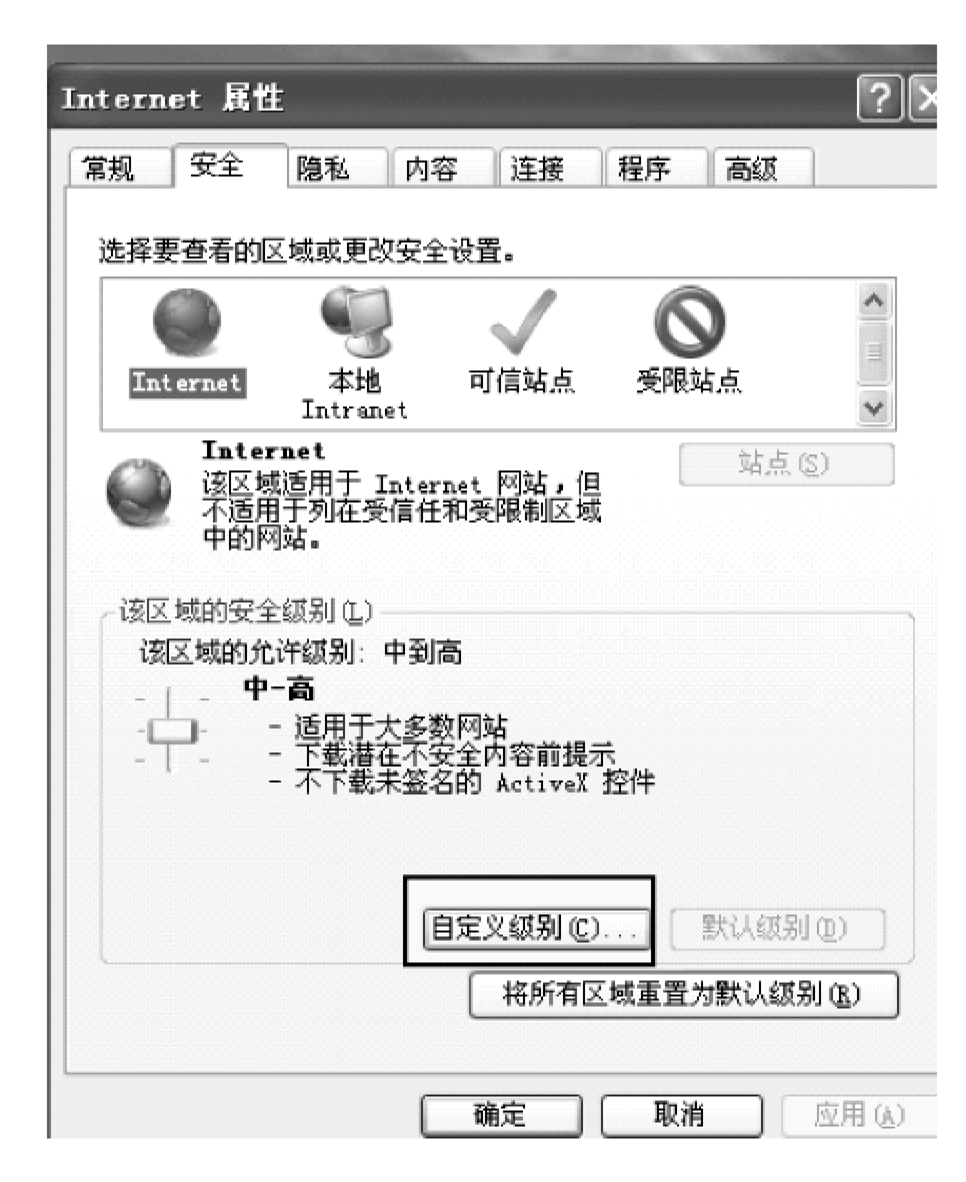


图 5.2　定义安全级别

5.2.4　蠕虫病毒案例

1. “熊猫烧香”病毒

“熊猫烧香”是一个由 Delphi 工具编写的蠕虫，终止大量的反病毒软件和防火墙软件进程。病毒会删除扩展名为 gho 的文件，使用户无法使用 ghost 软件恢复操作系统。“熊猫烧香”感染系统的. exe、. com、. pif、. src、. html、. asp 文件，添加病毒网址，导致用户一打开这些网页文件，IE 就会自动连接到指定的病毒网址中下载病毒。在硬盘各个分区下生成文件 autorun. inf 和 setup. exe，可以通过 U 盘和移动硬盘等方式进行传播，并且利用 Windows 系统的自动播放功能来运行，搜索硬盘中的. exe 可执行文件并感染，感染后的文件图标变成“熊猫烧香”图案，感染“熊猫烧香”病毒时的现象如图 5.3 所示。“熊猫烧香”还可以通过共享文件夹、系统弱口令等多种方式进行传播。

据瑞星反病毒专家介绍，“熊猫烧香”其实是“尼姆亚”病毒的新变种，最早出现在 2006 年的 11 月，由于它一直在不停地进行变种，而且该病毒会将中毒计算机中所有的网页文件尾部添加病毒代码，因此，一旦一些网站编辑人员的计算机被该病毒感染，网站编辑在上传网页到网站后，就会导致所有浏览该网页的计算机用户也被感染上该病毒。

同时，金山毒霸反病毒中心表示，“熊猫烧香”除了通过网站带毒感染用户之外，此病毒还会通过 QQ 最新漏洞传播，通过网络文件共享、默认共享、系统弱口令、U 盘及移动硬盘等多种途径传播。而局域网中只要有一台机器感染，就可以瞬间传遍整个网络，甚至在极短时间之内就可以感染几千台计算机，严重时可以导致网络瘫痪。中毒症状表现为计算机中所有可执行的. exe 文件都变成了一种怪异的图案，该图案显示为“熊猫烧香”，继而系统蓝屏、频繁重启、硬盘数据被破坏等，严重的整个公司局域网内所有计算机全部中毒。

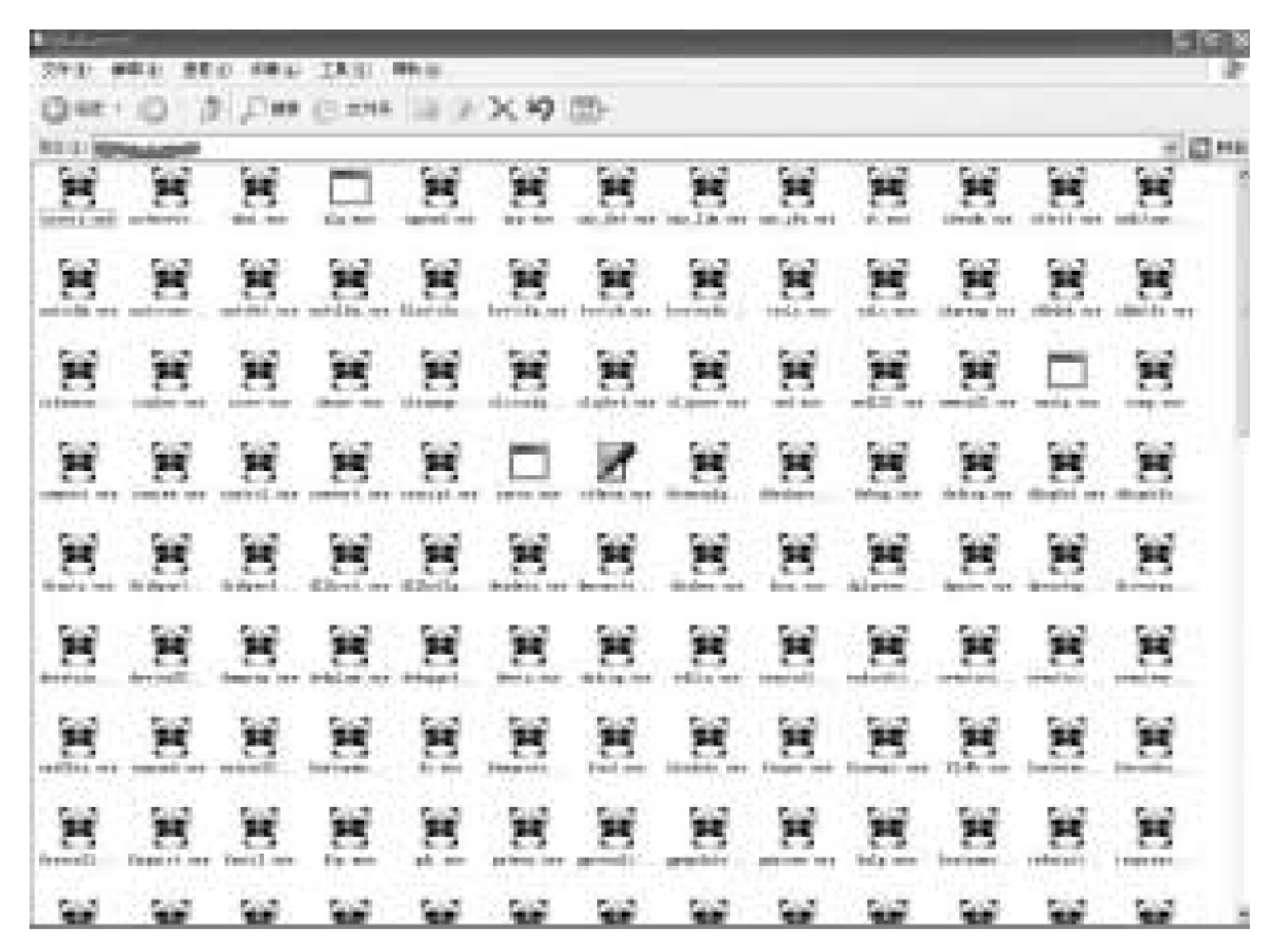


图 5.3　感染“熊猫烧香”病毒的现象

对此，江民反病毒专家分析认为：导致病毒快速传播目前存在三大原因：一是大量的企业用户使用国外杀毒软件，而国外杀毒软件对于此类国产病毒响应速度特别慢。二是由于被种植“熊猫烧香”病毒网站的点击量的全球排名均在前 300 名之列，而当一部分网站编辑本身机器感染了病毒之后，当他们把受感染文件上传到服务器后，访问者点击此类受感染网页即中毒，因此，该病毒才会得以迅速传播。三是其病毒具有极强的变种能力，仅从 2006 年 11 月至年底短短一个多月的时间，该病毒就变种将近 30 余次，因此在许多用户疏于防范而没有更新杀毒软件时，该病毒即可借机迅速传播。

预防“熊猫烧香”这类病毒的措施：

(1) 立即检查本机 administrator 组成员口令，一定要放弃简单口令甚至空口令，安全的口令是字母数字特殊字符的组合，自己记得住，别让病毒猜到就行。

修改方法：右键单击“我的计算机”，选择“管理”，浏览到“本地用户和组”，在右边的窗格中，选择具备管理员权限的用户名，单击右键，选择“设置密码”，输入新密码即可，如图 5.4 所示。

(2) 利用组策略，关闭所有驱动器的自动播放功能。

修改方法：选择“开始”→“运行”命令，输入 gpedit.msc，打开组策略编辑器，浏览到“计算机配置”→“管理模板”→“系统”，在右边的窗格中选择关闭自动播放，该配置默认是未配置，在下拉列表框中选择“所有驱动器”，再选取“已启用”，确定后关闭。最后，选择“开始”→“运行”命令，输入 gpupdate，确定后，该策略就生效了。

(3) 修改文件夹选项，以查看不明文件的真实属性，避免无意双击骗子程序中毒。

修改方法：打开资源管理器(按 Windows 徽标键＋E)，点工具菜单下文件夹选项，再点查看，在高级设置中，选择查看所有文件，取消隐藏受保护的操作系统文件，取消隐藏文件扩展名。

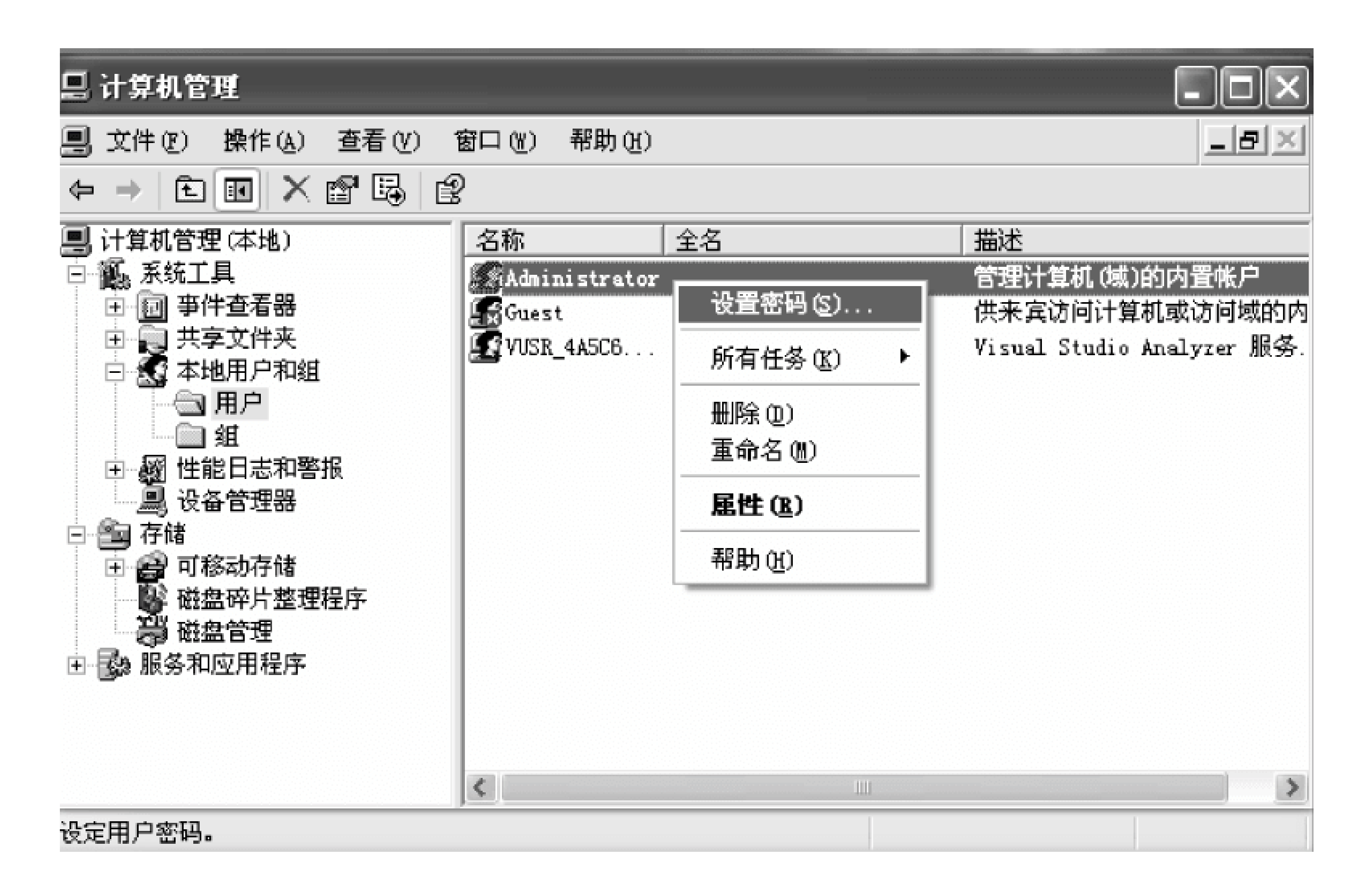


图 5.4 设置用户密码

(4) 时刻保持操作系统获得最新的安全更新,不要随意访问来源不明的网站,特别是微软的 MS06-014 漏洞,应立即打好该漏洞补丁。同时,QQ、MSN 的漏洞也可以被该病毒利用,因此,用户应该去相关的官方网站打好最新补丁。此外,由于该病毒会利用 IE 浏览器的漏洞进行攻击,因此用户还应该给 IE 打好所有的补丁。如果必要的话,用户可以暂时换用 Firefox、Opera 等比较安全的浏览器。

(5) 启用 Windows 防火墙保护本地计算机。局域网用户尽量避免创建可写的共享目录,已经创建共享目录的应立即停止共享。

此外,对于未感染的用户,病毒专家建议,不要登录不良网站,及时下载微软公布的最新补丁,来避免病毒利用漏洞袭击用户的计算机,同时上网时应采用"杀毒软件+防火墙"的立体防御体系。

2. "U 盘寄生虫"病毒

金山反病毒中心将该病毒统称为"AV 终结者",瑞星反病毒中心将该病毒称为"帕虫",江民反病毒中心将该病毒称为"U 盘寄生虫"。

"U 盘寄生虫"为一款利用 U 盘等移动存储设备传播的蠕虫病毒,通过网络大规模自动传播,传播方式包括电子邮件、网络共享、系统漏洞、即时通信软件等。"U 盘寄生虫"会利用 U 盘、MP3、移动硬盘等设备中的自动播放文件发作,大量占用系统资源,使计算机运行缓慢、无法上网,甚至导致系统瘫痪。此外,受到攻击的局域网还可能出现网络堵塞、瘫痪等严重症状。

"U 盘寄生虫"是蠕虫家族的重要成员之一,采用 Delphi 语言编写,并经过加壳处理。"U 盘寄生虫"运行后,自我复制到系统盘根目录下,文件名为"test. exe",将文件属性设置为隐藏,并在相同目录下创建"autorun. inf"文件,达到双击盘符就可启动"U 盘寄生虫"病毒的目的。普通用户一旦感染该病毒,从病毒进入计算机,到实施破坏,四步就可导致用户计算机彻底崩溃:第一步禁用所有杀毒软件及相关安全工具,让计算机失去安全保障;第二步破坏安全模式,致使用户根本无法进入安全模式清除病毒;第三步强行关闭带有病毒字样的网页,只要在网页中输入"病毒"相关字样,网页遂被强行关闭,即使是一些安全论坛也

无法登录，用户无法通过网络寻求解决办法；第四步格式化系统盘重装后很容易被再次感染。

用户格式化后，只要双击其他盘符，病毒将再次运行。此外，用户计算机的安全防御体系被彻底摧毁，安全性几乎为零，而“AV 终结者”自动连接到拥有病毒的网站，并下载数百种木马病毒，各类盗号木马、广告木马、风险程序在用户计算机毫无抵抗力的情况下，鱼贯而来，用户的网银、网游、QQ 账号密码以及机密文件都处于极度危险之中。因此提醒计算机用户目前使用计算机需慎之又慎。

瑞星反病毒中心目前将该病毒称为“帕虫”病毒。据瑞星反病毒中心表示：“该病毒采用了多种技术手段来保护自身不被清除，例如，它会终结几十种常用的杀毒软件，如果用户使用 google、百度等搜索引擎搜索‘病毒’，浏览器也会被病毒强制关闭，使得用户无法取得相关信息。尤为恶劣的是，该病毒还采用了 IFEO 劫持（Windows 文件映像劫持）技术，修改注册表，使 QQ 医生、360 安全卫士等几十种常用软件无法正常运行，从而使得用户很难手工清除该病毒。”

此外，据反病毒专家介绍：“该病毒通过映像劫持技术，将大量杀毒软件‘绑架’，使其无法正常应用，而用户在点击相关安全软件后，实际上已经运行了病毒文件，实现病毒的‘先劫持后掉包’的计划。该病毒不但可以劫持大量杀毒软件以及安全工具，而且还可禁止 Windows 的自更新和系统自带的防火墙，大大降低了用户系统的安全性，这也是近几年来对用户的系统安全破坏程度最大的病毒之一。而且该病毒还会在每个磁盘分区上建立自动运行文件（包括 U 盘），从而使得通过 U 盘传播的概率大大增加。同时，由于每个分区上都有病毒留下的文件，普通用户即使格式化 C 盘重装系统，也无法彻底清除该病毒。”

病毒专家建议，计算机用户应及时升级杀毒软件，开启杀毒软件“实时监控”和“系统监测”功能，防范已知和未知病毒。针对越来越多的病毒通过 U 盘传播特征，专家建议用户在使用 U 盘前，务必先使用杀毒软件进行扫描，确认无毒后再打开。此外，用户应养成良好的安全习惯，不随意点击不明链接和运行不明文件，及时为操作系统打好补丁，关闭系统共享以及为系统设置复杂的口令，都可有效减少病毒侵害。

5.2.5 病毒、木马、蠕虫比较

通过网络传播的病毒不是网络病毒。只有蠕虫等一些威胁可以算作网络病毒。蠕虫病毒也不是普通病毒所能比拟的，网络的发展使得蠕虫可以在短短的时间内蔓延整个网络，造成网络瘫痪。表 5.1 列出了病毒、木马、蠕虫的各自特点和区别，便于大家理解。

表 5.1 病毒、木马、蠕虫比较

	计算机病毒	特洛伊木马	计算机蠕虫
感染其他档案	会	不会	不会
被动散播自己	是	是	不是
主动散播自己	不是	不是	是
造成程序增加数目	计算机使用率愈高，档案受感染的数目愈多	不会增加	取决于网路连接情况，范围愈广，散布的数目愈多
破坏力	取决于病毒作者	取决于病毒作者	无
对企业的影响	中	低	高

网络用户所受网络攻击类型统计如图 5.5 所示，计算机病毒、蠕虫和木马程序造成的安全事件占发生安全事件单位总数的 79%；拒绝服务、端口扫描和篡改网页等网络攻击事件占 43%；大规模垃圾邮件传播造成的安全事件占 36%；54%的被调查单位网络安全事件造成的损失比较轻微；损失严重和非常严重的占发生安全事件单位总数的 10%。

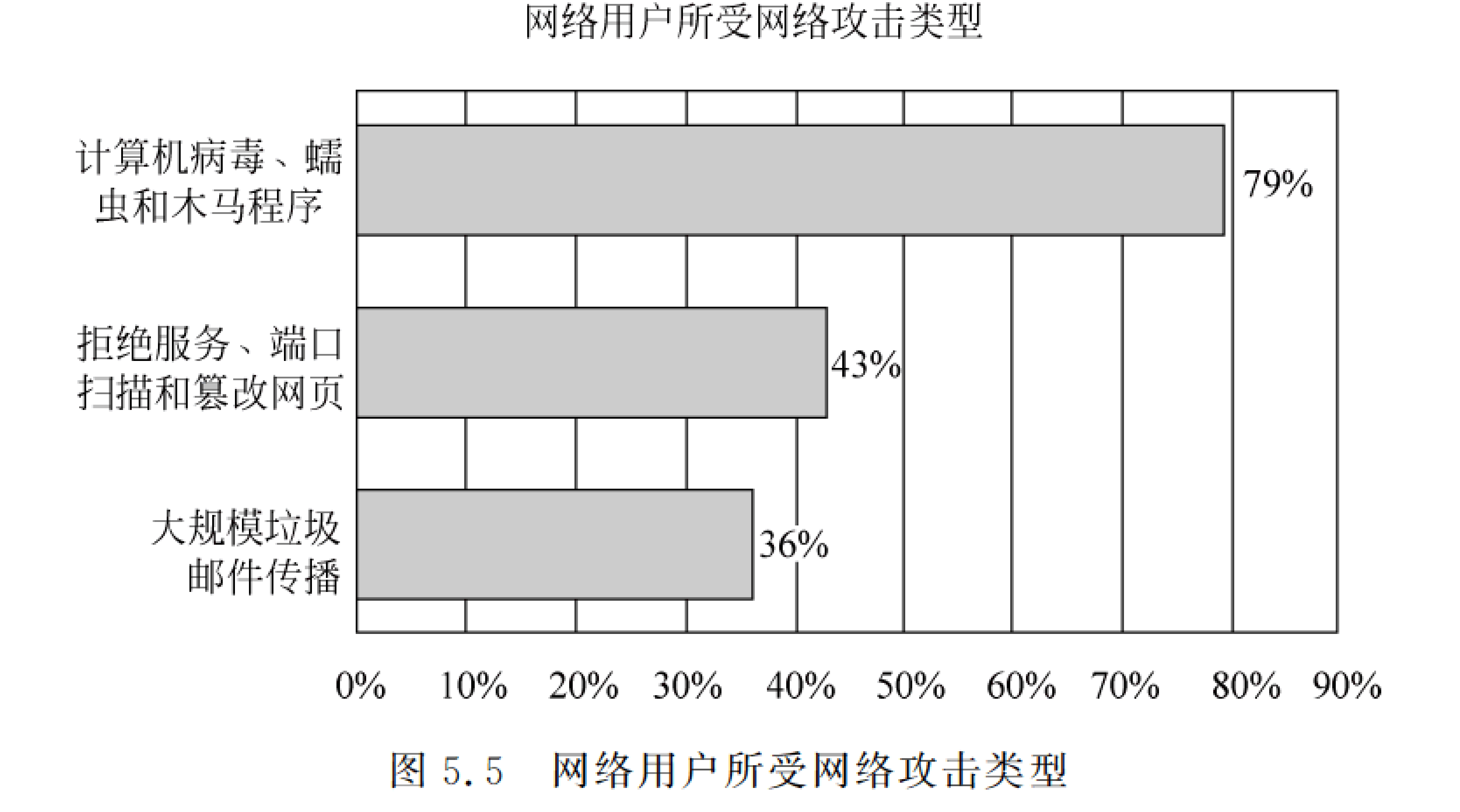


图 5.5 网络用户所受网络攻击类型

5.2.6 网络病毒的发展趋势

随着网络的发展，网络病毒呈现出一些新的发展趋势，主要有以下几点：

(1) 传播介质与攻击对象多元化，传播速度更快，覆盖面更广。网络病毒的传播不仅可利用磁介质，更多的是通过各种通信端口、网络和邮件等迅速传播。攻击对象由单一的个人计算机变为所有具备通信功能的工作站、服务器甚至掌上型移动通信工具和 PDA。

(2) 破坏性更强。网络病毒的破坏性日益增强，它们可以造成网络拥塞、进而瘫痪，重要数据丢失，机密信息失窃，甚至通过病毒完全控制计算机信息系统和网络。

(3) 难以控制和根治。在网络中，只要有一台计算机感染病毒，就可通过内部机制进行传播，很快使整个网络受到影响甚至拥塞或瘫痪。

(4) 病毒携带形式多样化。在网络环境下，可执行程序、脚本文件、HTML 网页、电子邮件、网上贺卡甚至卡通图片等都有可能携带计算机病毒。

(5) 编写方式多样化，病毒变种多。网络环境下除了传统的汇编语言、C 语言等，以 JavaScript 和 VBScript 为首的脚本语言已成为最流行的病毒语言。利用新的编程语言与编程技术实现的病毒更易于被修改以产生新的变种，从而逃避反病毒软件的检查。另外，已经出现了专门生产病毒的病毒生产机程序，使得新病毒出现的频率大大提高。

(6) 触发条件增多，感染与发作的几率增大。

(7) 智能化，隐蔽化。目前网络病毒常常用到隐形技术、反跟踪技术、加密技术、自变异技术、自我保护技术、针对某种反病毒技术的反措施技术以及突破计算机网络防护措施的技术等，这使得网络环境下的病毒更加智能化、隐蔽化。

(8) 攻击目的明确化。一些高级病毒出于某种经济或政治上的目的，被研制出来扰乱或破坏社会信息、政治、经济秩序，甚至是作为一种信息战略武器。

5.3　病毒检测技术

随着计算机病毒技术的不断发展，检测和查杀计算机病毒的技术也在不断地更新并趋于复杂化和智能化。为了选取有效的病毒检测技术，在这一部分，首先将对传统的病毒诊断技术进行分析和对比，其次对基于网络的病毒检测技术进行分析。

5.3.1　传统的病毒检测技术

1. 程序和数据完整性检测技术

完整性病毒检测技术是一种相当古老的病毒检测方法。它的基本原理是对每个程序或者代码根据某种算法生成校验码（提取签名），一旦程序发生变化，所产生的校验码必然与原来生成的校验码不同，这时，可以初步判断该改程序已经被病毒感染。这种技术具有很多弱点，以至于现在几乎不被采用了。其中包括，病毒检测软件需要建立一个统一的校验码库，不能对经常发生变化的数据文件进行检测和保护。有时，程序被改动并不是病毒感染造成的，从而造成检测的误报率相当高。这种检测方法不能明确地判定病毒的具体类型，而且，如果程序在生成校验码前已经被病毒感染，则逃脱了以后的完整性检测。

2. 病毒特征码检测技术

病毒特征码检测技术是目前被广泛使用的一种病毒检测技术。它的基本原理是通过对病毒源程序的分析，提取出能够唯一代表该病毒的一串病毒代码，该串代码经过测试，是其他程序所没有的。这种病毒检测的方法，非常高效，如果病毒特征码提取质量高的话，病毒的检测率相当高，而误报率会非常小。这种病毒检测方法能够唯一地确定病毒的种类和名字，为下一步的杀毒提供依据。这种检测技术的弱点是，它仅仅能够检测已知病毒，而对于未知病毒往往需要经过人工分析，提取特征码后才能进行。随着病毒技术的不断发展，特别是变形病毒的出现，病毒每次传染后病毒代码本身都会加密而各次代码都不相同。这时，就不存在一个单一的病毒特征码了，所以病毒特征码检测技术对变形病毒可以说是无能为力。

3. 启发式规则（或广谱特征码）病毒检测技术

启发式规则病毒检测是一种专门针对未知病毒的病毒检测技术。它的基本原理是通过对一系列病毒代码的分析，提取一种广谱特征码，即代表病毒的某一种行为特征的特殊程序代码，当然仅仅是一段特征码还不能确定一定是某一种病毒，通过多种广谱特征码，也就是启发式规则的判断，综合考虑各种因素，确定到底是否是病毒，是哪一种病毒。这种病毒检测方法的优点就是针对未知病毒，而缺点在于，它的诊断的正确率（包括检测率和误报率）和规则的选取有密切的关系。往往是某些规则对某种病毒很有效，但是却影响其他类型的病毒的检测。规则选取的困难和相互矛盾决定了这种方法只能是一种辅助的检测手段。

4. 基于操作系统的监视和检测技术

较早的操作系统监视和检测技术是从中断向量监视开始的，病毒诊断软件通过监视系统的中断向量表来判定是否有病毒入侵。此外，内存检测也是操作系统检测技术的手段之一。随着技术的不断发展，现在的一些杀毒产品采用的是嵌入操作系统内核的检测，它不仅检测中断向量表等一些关键数据结构，还要监视系统的一些关键调用、系统的运行状况、文件系统的访问状况等多个指标，从而判定系统是否工作不正常，程序是否被病毒感染。这种

监视和检测技术的实现难度很大，需要操作系统厂商的配合。而且，这种方法同样无法确定究竟是何种病毒，误报率很高。

5. 传统虚拟机病毒检测技术

虚拟机病毒检测技术是一种最新的病毒检测技术。它的基本原理是，为可能的病毒程序构建一个虚拟的运行环境，诱使病毒程序进行感染和破坏活动。虚拟机病毒检测技术的最大优点是能够很高效率地检测出病毒，特别是特征码技术很难解决的变形病毒技术。早期的虚拟机并不是真正意义上的虚拟机，它们仅仅是利用 Windows 操作系统的一些特殊功能来构造一个伪虚拟机，但是聪明的病毒程序往往可以破坏虚拟机本身。而且，虚拟机的运行需要相当的系统资源，可能会影响正常程序的运行。

通过对以上技术的比较，可以看出，无论哪一种技术都不能说是十全十美的。就目前计算机病毒的诊断技术而言，无论是哪一种诊断软件都不可能仅仅采用某一种诊断方法。最新的病毒诊断技术往往把多种技术融合在一起，发挥各种技术的长处，达到最好的效果。

5.3.2 基于网络的病毒检测技术

从本质上讲，基于网络的病毒检测技术并没有在传统的病毒检测技术上做出本质性的更新，新的技术往往是针对网络病毒的特点，对传统的病毒监测技术进行优化并应用在网络环境中。

1. 实时网络流量检测

从原理上，实时网络流量监测继承了自病毒特征码检测技术，但是网络病毒检测有其独到之处。网络病毒的实时检测将实时地截取网络文件传输的信息流，从传播途径上对病毒进行及时的检测，并能够实时做出反馈行为。网络病毒实时检测的目标是已知的病毒。其优点在于它能实时地监测网络流量，发现绝大多数已知病毒，缺点在于随着网络流量的呈几何级数增长，对巨大的流量进行实时监测往往需要占用大量的系统资源，同时对未知病毒，这种方法完全无能为力。在我们的系统中，也使用了实时的网络流量监测，并针对它存在的缺陷进行了改进和完善。

2. 异常流量分析

网络流量异常的种类较多，从不同的角度分析有不同的分类结果，从产生异常流量的原因分析可以将其分成三个广义的异常类：网络操作异常、闪现拥挤异常和网络滥用异常。网络操作异常是指网络设备的停机、配置改变等导致的网络行为的显著变化，以及流量达到环境极限引起的台阶行为；闪现拥挤异常出现的原因通常是软件版本的问题，或者是国家公开带来的 Web 站点的外部利益问题。特定类型流量的快速增长（例如 FTP 流），或者知名 IP 地址的流量随着时间渐渐降低，都是闪现拥挤的显著表现；网络滥用异常主要是由以 DoS 洪泛攻击和端口扫描为代表的各种网络攻击导致的，这种网络异常也是我们的网络病毒检测系统所感兴趣的。

基于网络滥用异常的流量分析可以看作是对启发式规则病毒检测技术的一种衍生，这种技术的优势是能发现未知的网络病毒，同时可以通过流量信息直接定位可能感染了病毒的机器，对于一些蠕虫的变种及新的网络病毒有较好的发现效果。

3. 蜜罐系统

蜜罐系统可以看做是传统的虚拟机病毒检测技术在网络环境中的一种新的应用。蜜罐定义为一种安全资源,它并没有任何业务上的用途,它的价值就是吸引攻击者对它进行非法的使用。蜜罐技术本质上是一种对攻击者进行欺骗的技术,通过布置一些作为诱饵的主机、网络服务以及信息诱使攻击者对其进行攻击,减少对实际系统所造成的安全威胁。更重要的是蜜罐技术可以对攻击行为进行监控和分析,了解攻击者所使用的攻击工具和攻击方法,推测攻击者的意图和动机,在此基础上尽可能地追踪攻击者的来源,对其攻击行为进行审计和取证,从而能够让防御者清晰地了解他们所面对的安全威胁,并通过法律手段去追究攻击者的责任,或者通过技术和管理手段来增强对实际系统的安全防护能力。蜜罐技术最大的应用目标是提供一个高度可控的环境对互联网上的各种安全威胁(包括黑客攻击、恶意软件传播、垃圾邮件、僵尸网络和网络钓鱼等)进行深入的了解与分析,从而为安全防御提供知识和经验支持。

课 后 习 题

选择题

1. 不属于计算机病毒防治策略的是(　　)。

A. 确认您手头常备一张真正“干净”的引导盘

B. 及时、可靠升级反病毒产品

C. 新购置的计算机软件也要进行病毒检测

D. 整理磁盘

2. 计算机病毒的特征之一是(　　)。

A. 非授权不可执行性　　B. 非授权可执行性

C. 授权不可执行性　　D. 授权可执行性

3. 计算机病毒最重要的特征是(　　)。

A. 隐蔽性　　B. 传染性　　C. 潜伏性　　D. 破坏性

4. 计算机病毒(　　)。

A. 不影响计算机的运算速度　　B. 可能会造成计算机器件的永久失效

C. 不影响计算机的运算结果　　D. 不影响程序执行. 破坏数据与程序

5. CIH 病毒破坏计算机的 BIOS,使计算机无法启动。它是由时间条件来触发的,其发作的时间是每月的 26 号,这主要说明病毒具有(　　)。

A. 可传染性　　B. 可触发性　　C. 破坏性　　D. 免疫性

填空题

1. 网络病毒主要进行游戏等(　　)的盗取工作,远程操控,或把你的计算机当作肉鸡使用。

2. 特洛伊木马简称木马,它是一种基于(　　)的黑客工具,具有(　　)和(　　)的特点。

3. 蠕虫程序主要利用(　　)进行传播。

4. 蠕虫病毒采取的传播方式,一般为(　　)以及(　　)。

5.（　　）可以阻挡90%的黑客、蠕虫病毒及消除系统漏洞引起的安全性问题。

简答题

1. 什么是计算机病毒?
2. 什么是木马?
3. 什么是蠕虫?
4. 计算机病毒的特点有哪些?
5. 用户计算机中毒症状有哪些?
6. 网络传播性木马有哪些新的特征?
7. 蠕虫的行为特征有哪些?
8. 蠕虫技术发展的趋势是什么?
9. 网络病毒的发展趋势有哪几点?
10. 个人用户对蠕虫病毒的防范措施有哪些?
11. 防范“熊猫烧香”病毒的措施有哪些?
12. 病毒检测技术主要有哪些种类?

第6章　防火墙技术

6.1　防火墙概述

所谓防火墙指的是一个由软件和硬件设备组合而成、在内部网和外部网之间、专用网与公共网之间的界面上构造的保护屏障，是一种获取安全性方法的形象说法，它是一种计算机硬件和软件的结合，使 Internet 与 Intranet 之间建立起一个安全网关，从而保护内部网免受非法用户的侵入。防火墙主要由服务访问规则、验证工具、包过滤和应用网关 4 个部分组成。防火墙结构示意图如图 6.1 所示。计算机流入流出的所有网络通信均要经过此防火墙。

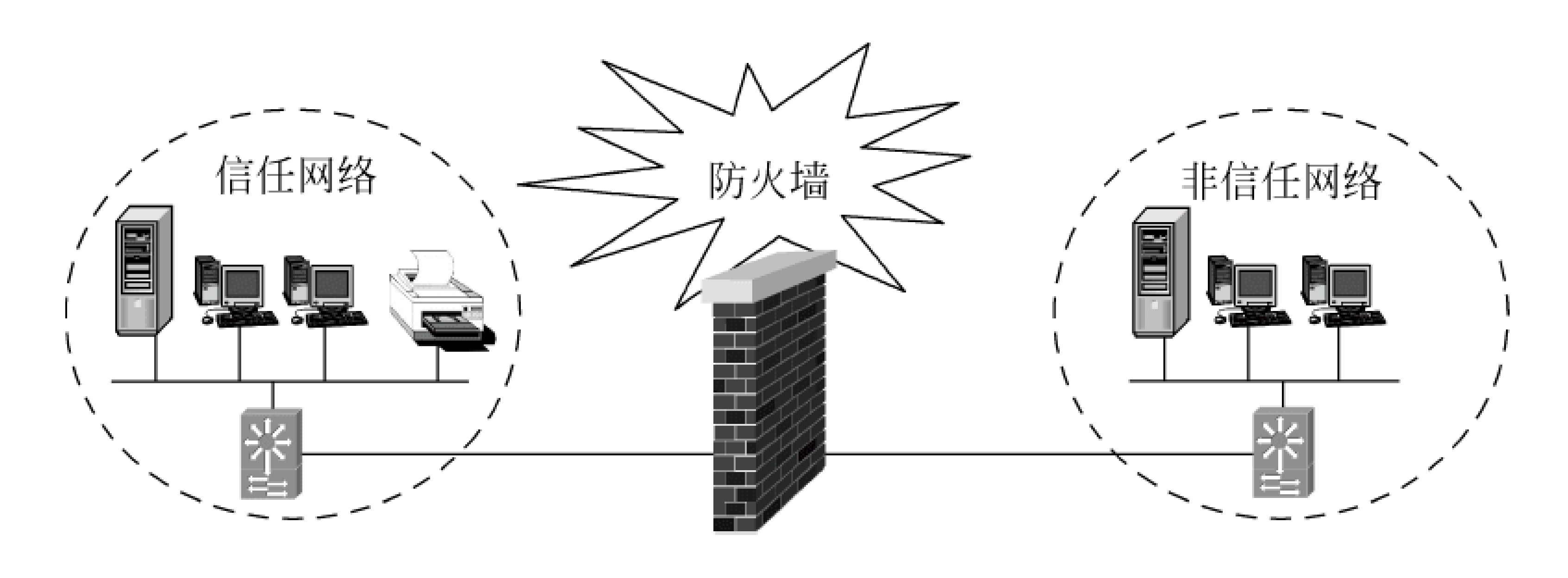


图 6.1　防火墙示意图

6.1.1　防火墙的功能

防火墙在网络中真正像一堵墙一样。从防火墙的过滤机制来说，防火墙就像一个二极管一样，而二极管具有单向导电性，这样也就形象地说明了防火墙具有单向导通性。这看起来与现在防火墙过滤机制有些矛盾，不过它却完全体现了防火墙初期的设计思想，同时也在相当大程度上体现了当前防火墙的过滤机制。因为防火墙最初的设计思想是对内部网络总是信任的，而对外部网络却总是不信任的，所以最初的防火墙是只对外部进来的通信进行过滤，而对内部网络用户发出的通信不作限制。当然目前的防火墙在过滤机制上有所改变，不仅对外部网络发出的通信连接要进行过滤，对内部网络用户发出的部分连接请求和数据包同样需要过滤，但防火墙仍只允许符合安全策略的通信通过，也可以说具有单向导通性。

防火墙的原意是指古代构筑和使用木制结构房屋的时候，为防止火灾的发生和蔓延，人们将坚固的石块堆砌在房屋周围作为屏障，这种防护构筑物就被称为“防火墙”。其实与防火墙一起起作用的就是“门”。如果没有门，各房间的人如何沟通呢？这些房间的人又如何进去呢？当火灾发生时，这些人又如何逃离现场呢？这个门就相当于这里所讲的防火墙的

"安全策略"，所以在此处所说的防火墙实际上并不是一堵实心墙，而是带有一些小孔的墙。这些小孔就是用来留给那些允许进行的通信，在这些小孔中安装了过滤机制，也就是上面所介绍的单向导通性。

防火墙的功能可以归纳为以下几个方面。

1. 防火墙是网络安全的屏障

一个防火墙(作为阻塞点、控制点)能极大地提高一个内部网络的安全性，并通过过滤不安全的服务而降低风险。由于只有经过精心选择的应用协议才能通过防火墙，所以网络环境变得更安全。如防火墙可以禁止诸如众所周知的不安全的 NFS 协议进出受保护网络，这样外部的攻击者就不可能利用这些脆弱的协议来攻击内部网络。防火墙同时可以保护网络免受基于路由的攻击，如 IP 选项中的源路由攻击和 ICMP 重定向中的重定向路径。防火墙应该可以拒绝所有以上类型攻击的报文并通知防火墙管理员。

2. 防火墙可以强化网络安全策略

通过以防火墙为中心的安全方案配置，能将所有安全软件(如口令、加密、身份认证、审计等)配置在防火墙上。与将网络安全问题分散到各个主机上相比，防火墙的集中安全管理更经济。例如在网络访问时，动态口令系统和其他身份认证系统完全可以不必分散在各个主机上，而集中在防火墙上。

3. 对网络存取和访问进行监控审计

如果所有的访问都经过防火墙，那么，防火墙就能记录下这些访问并作出日志记录，同时也能提供网络使用情况的统计数据。当发生可疑动作时，防火墙能进行适当的报警，并提供网络是否受到监测和攻击的详细信息。另外，收集一个网络的使用和误用情况也是非常重要的。首先的理由是可以清楚防火墙是否能够抵挡攻击者的探测和攻击，并且清楚防火墙的控制是否充足。而网络使用情况的统计对网络需求分析和威胁分析等而言也是非常重要的。

4. 防止内部信息的外泄

通过利用防火墙对内部网络的划分，可实现内部网重点网段的隔离，从而限制了局部重点或敏感网络安全问题对全局网络造成的影响。再者，隐私是内部网络非常关心的问题，一个内部网络中不引人注意的细节可能包含了有关安全的线索而引起外部攻击者的兴趣，甚至因此而暴露了内部网络的某些安全漏洞。使用防火墙就可以隐蔽那些透漏内部细节如 Finger、DNS 等服务。Finger 显示了主机的所有用户的注册名、真名，最后登录时间和使用 shell 类型等。但是 Finger 显示的信息非常容易被攻击者所获悉。攻击者可以知道一个系统使用的频繁程度，这个系统是否有用户正在连线上网，这个系统是否在被攻击时引起注意等。防火墙可以同样阻塞有关内部网络中的 DNS 信息，这样一台主机的域名和 IP 地址就不会被外界所了解。

除了安全作用，防火墙还支持具有 VPN(虚拟专用网)、NAT(网络地址转换)等功能。

6.1.2 防火墙的基本特性

防火墙可以使企业内部局域网网络与 Internet 之间或者与其他外部网络互相隔离、限制网络互访用来保护内部网络。典型的防火墙具有以下三个方面的基本特性。

1. 内部网络和外部网络之间的所有网络数据流都必须经过防火墙

这是防火墙所处网络位置决定的，同时也是一个前提。因为只有当防火墙是内、外部网络之间通信的唯一通道，才可以全面、有效地保护企业内部网络不受侵害。

根据美国国家安全局制定的《信息保障技术框架》，防火墙适用于用户网络系统的边界，属于用户网络边界的安全保护设备。网络边界是采用不同安全策略的两个网络连接处，比如用户网络和互联网之间连接、与其他业务往来单位的网络连接、用户内部网络不同部门之间的连接等。防火墙的目的就是在网络连接之间建立一个安全控制点，通过允许、拒绝或重新定向经过防火墙的数据流，实现对进、出内部网络的服务和访问的审计和控制。

典型的防火墙体系结构如图6.2所示。从图中可以看出，防火墙的一端连接企事业单位内部的局域网，而另一端则连接着互联网。所有的内、外部网络之间的通信都要经过防火墙。而内部网络之间也可通过安全防火墙来实现数据流的控制。

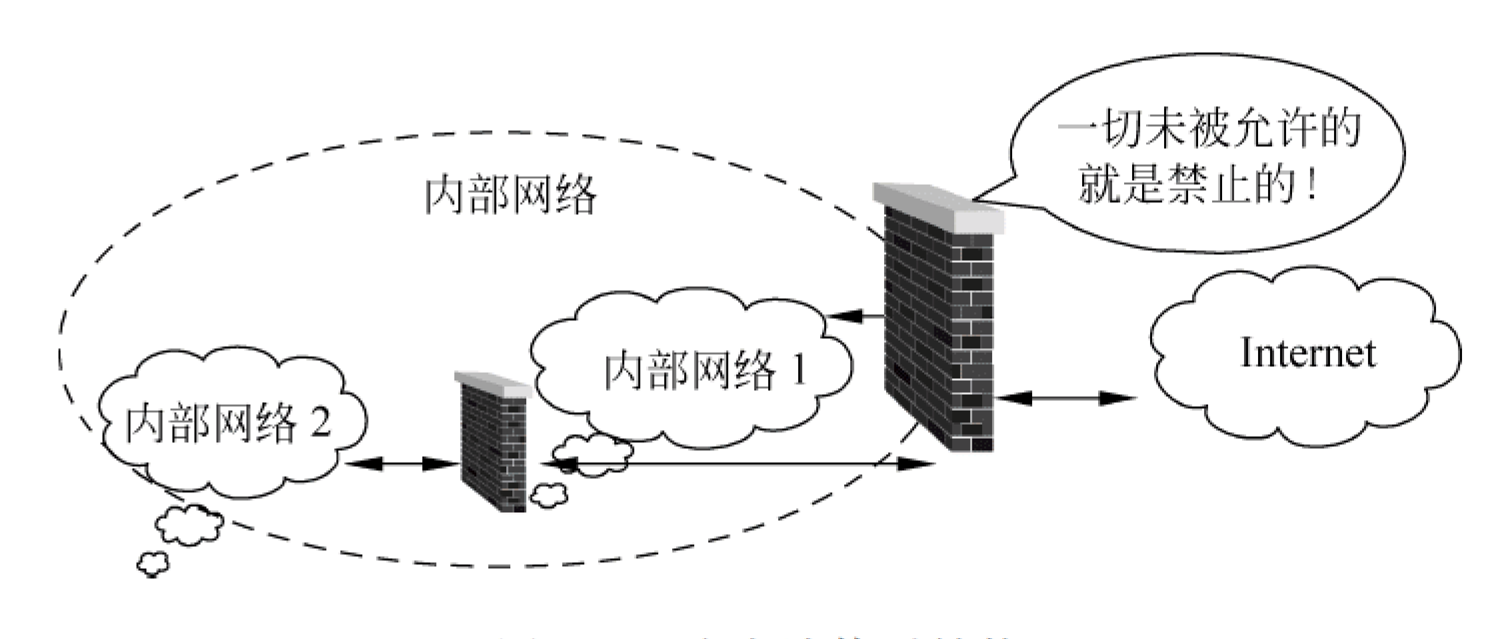


图6.2 防火墙体系结构

2. 只有符合安全策略的数据流才能通过防火墙

防火墙最基本的功能是确保网络流量的合法性，并在此前提下将网络的流量快速地从一条链路转发到另外的链路上去。从最早的防火墙模型开始谈起，原始的防火墙是一台“双穴主机”，即具备两个网络接口，同时拥有两个网络层地址。防火墙将网络上的流量通过相应的网络接口接收上来，按照OSI协议栈的七层结构顺序上传，在适当的协议层进行访问规则和安全审查，然后将符合通过条件的报文从相应的网络接口送出，而对于那些不符合通过条件的报文则予以阻断。因此，从这个角度上来说，防火墙是一个类似于桥接或路由器的、多端口的（网络接口≥2）转发设备，它跨接于多个分离的物理网段之间，并在报文转发过程之中完成对报文的审查工作。

3. 防火墙自身应具有非常强的抗攻击免疫力

这是防火墙之所以能担当企业内部网络安全防护重任的先决条件。防火墙处于网络边缘，它就像一个边界卫士一样，每时每刻都要面对黑客的入侵，这样就要求防火墙自身要具有非常强的抗击入侵本领。它之所以具有这么强的本领，防火墙操作系统本身是关键，只有自身具有完整信任关系的操作系统才可以谈论系统的安全性。其次就是防火墙自身具有非常低的服务功能，除了专门的防火墙嵌入系统外，再没有其他应用程序在防火墙上运行。当然这些安全性也只能说是相对的。

目前国内的防火墙几乎被国外的品牌占据了一半的市场，国外品牌的优势主要是在技术和知名度上比国内产品高；而国内防火墙厂商对国内用户了解更加透彻，价格上也更具有优势。防火墙产品中，国外主流厂商为Cisco、CheckPoint、NetScreen等，国内主流厂商为

东软、天融信、联想、方正等,它们都提供不同级别的防火墙产品。

6.2 DMZ 简介

6.2.1 DMZ 的概念

DMZ 是英文 DeMilitarized Zone 的缩写,中文名称为“隔离区”,也称“非军事化区”。它是为了解决安装防火墙后外部网络不能访问内部网络服务器的问题,而设立的一个非安全系统与安全系统之间的缓冲区,这个缓冲区位于企业内部网络和外部网络之间的小网络区域内,在这个小网络区域内可以放置一些必须公开的服务器设施,如企业 Web 服务器、FTP 服务器和论坛等。另一方面,通过这样一个 DMZ 区域,更加有效地保护了内部网络,因为这种网络部署,比起一般的防火墙方案,对攻击者来说又多了一道关卡,如图 6.3 所示。

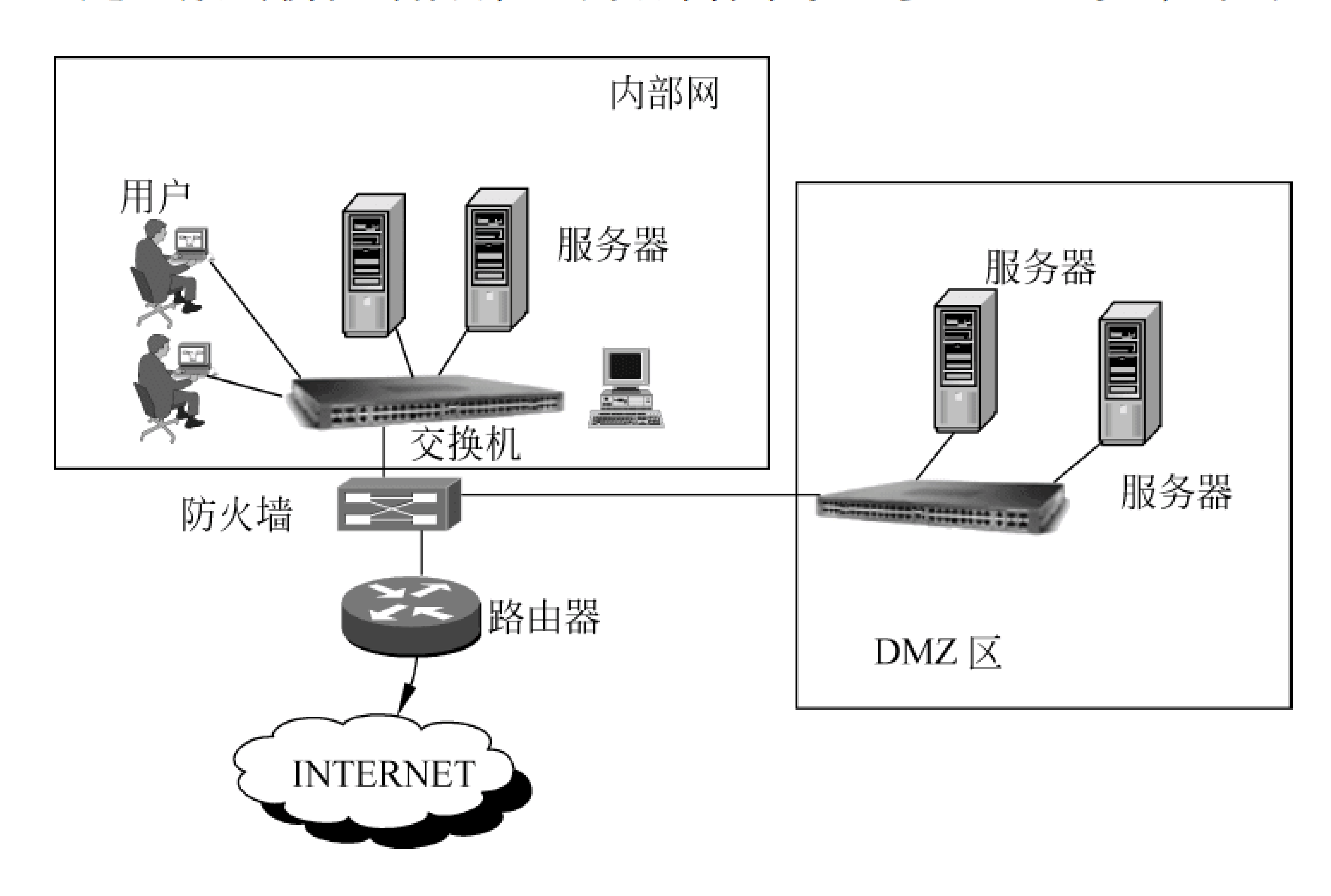


图 6.3 DMZ 示意图

网络设备开发商利用这一技术,开发出了相应的防火墙解决方案,称为“非军事区结构模式”。DMZ 通常是一个过滤的子网,在内部网络和外部网络之间构造了一个安全地带。

DMZ 防火墙方案为要保护的内部网络增加了一道安全防线,通常认为是非常安全的。同时它提供了一个区域放置公共服务器,从而又能有效地避免一些互联应用需要公开,却与内部安全策略相矛盾的情况发生。在 DMZ 区域中通常包括堡垒主机、modem 池,以及所有的公共服务器,但要注意的是电子商务服务器只能用作用户连接,真正的电子商务后台数据需要放在内部网络中。

在这个防火墙方案中,包括两个防火墙,外部防火墙抵挡外部网络的攻击,并管理所有内部网络对 DMZ 的访问。内部防火墙管理 DMZ 对于内部网络的访问。内部防火墙是内部网络的第三道安全防线(前面有了外部防火墙和堡垒主机),当外部防火墙失效的时候,它还可以起到保护内部网络的功能。而局域网内部,对于 Internet 的访问由内部防火墙和位于 DMZ 的堡垒主机控制。在这样的结构里,一个黑客必须通过三个独立的区域(外部防火墙、内部防火墙和堡垒主机)才能够到达局域网。攻击难度大大加强,相应内部网络的安全性也就大大加强,但投资成本也是最高的。

如果你的机器不提供网站或其他的网络服务的话不要设置。DMZ 是把你计算机的所有端口开放到网络。

6.2.2 DMZ 网络访问控制策略

当规划一个拥有 DMZ 的网络的时候，可以明确各个网络之间的访问关系，以确定以下6条访问控制策略。

(1) 内网可以访问外网，内网的用户显然需要自由地访问外网。在这一策略中，防火墙需要进行源地址转换。

(2) 内网可以访问 DMZ，此策略是为了方便内网用户使用和管理 DMZ 中的服务器。

(3) 外网不能访问内网，很显然，内网中存放的是公司内部数据，这些数据不允许外网的用户进行访问。

(4) 外网可以访问 DMZ，DMZ 中的服务器本身就是要给外界提供服务的，所以外网必须可以访问 DMZ。同时，外网访问 DMZ 需要由防火墙完成对外地址到服务器实际地址的转换。

(5) DMZ 不能访问内网，很明显，如果违背此策略，则当入侵者攻陷 DMZ 时，就可以进一步进攻到内网的重要数据。

(6) DMZ 不能访问外网，此条策略也有例外，比如 DMZ 中放置邮件服务器时，就需要访问外网，否则将不能正常工作。在网络中，非军事化区(DMZ)是指为不信任系统提供服务的孤立网段，其目的是把敏感的内部网络和其他提供访问服务的网络分开，阻止内网和外网直接通信，以保证内网安全。

6.2.3 DMZ 服务配置

DMZ 提供的服务是经过了网络地址转换(NAT)和受安全规则限制的，以达到隐蔽真实地址、控制访问的功能。首先要根据将要提供的服务和安全策略建立一个清晰的网络拓扑，确定 DMZ 区应用服务器的 IP 和端口号以及数据流向。通常网络通信流向为禁止外网区与内网区直接通信，DMZ 区既可与外网区进行通信，也可以与内网区进行通信，受安全规则限制。

1. 网络地址转换(NAT)

DMZ 区服务器与内网区、外网区的通信是经过网络地址转换实现的。网络地址转换用于将一个地址域(如专用 Intranet)映射到另一个地址域(如 Internet)，以达到隐藏专用网络的目的。DMZ 区服务器对内服务时映射成内网地址，对外服务时映射成外网地址。采用静态映射配置网络地址转换时，服务用 IP 和真实 IP 要一一映射，源地址转换和目的地址转换都必须要有。

2. DMZ 安全规则制定

安全规则集是安全策略的技术实现，一个可靠、高效的安全规则集是实现一个成功、安全的防火墙的非常关键的一步。如果防火墙规则集配置错误，再好的防火墙也只是摆设。在建立规则集时必须注意规则次序，因为防火墙大多以顺序方式检查信息包，同样的规则，以不同的次序放置，可能会完全改变防火墙的运转情况。如果信息包经过每一条规则而没有发现匹配，这个信息包便会被拒绝。一般来说，通常的顺序是，较特殊的规则在前，较普通

的规则在后，防止在找到一个特殊规则之前一个普通规则便被匹配，避免防火墙被配置错误。

DMZ 安全规则指定了非军事区内的某一主机（IP 地址）对应的安全策略。由于 DMZ 区内放置的服务器主机将提供公共服务，其地址是公开的，可以被外部网的用户访问，所以正确设置 DMZ 区安全规则对保证网络安全是十分重要的。

防火墙可以根据数据包的地址、协议和端口进行访问控制。它将每个连接作为一个数据流，通过规则表与连接表共同配合，对网络连接和会话的当前状态进行分析和监控。其用于过滤和监控的 IP 包信息主要有：源 IP 地址、目的 IP 地址、协议类型（IP、ICMP、TCP、UDP）、源 TCP/UDP 端口、目的 TCP/UDP 端口、ICMP 报文类型域和代码域、碎片包和其他标志位（如 SYN、ACK 位）等。

为了让 DMZ 区的应用服务器能与内网中服务器通信，需增加 DMZ 区安全规则，这样一个基于 DMZ 的安全应用服务便配置好了。其他的应用服务可根据安全策略逐个配置。

DMZ 无疑是网络安全防御体系中的重要组成部分，再加上入侵检测和基于主机的其他安全措施，将极大地提高公共服务及整个系统的安全性。

6.3 防火墙的技术发展历程

6.3.1 第一代防火墙：基于路由器的防火墙

由于多数路由器中本身就包含有分组过滤功能，故网络访问控制可通过路由控制来实现，从而使具有分组过滤功能的路由器成为第一代防火墙产品。

1. 基于路由器防火墙的特点

（1）利用路由器本身对分组的解析，以访问控制表方式实现对分组的过滤。

（2）过滤判决的依据可以是 IP 地址、端口号及其他网络特征。

（3）只有分组过滤功能，且防火墙与路由器是一体的，对安全要求低的网络采用路由器附带防火墙功能的方法，对安全性要求高的网络则可单独利用一台路由器作为防火墙。

2. 基于路由器防火墙的不足

（1）本身具有安全漏洞，外部网络要探寻内部网络十分容易。例如，在使用 FTP 协议时，外部服务器容易从 21 端口上与内部网相连，即使在路由器上设置了过滤规则，内部网络的 21 端口仍可由外部探寻。

（2）分组过滤规则的设置和配置存在安全隐患。对路由器中过滤规则的设置和配置十分复杂，它涉及规则的逻辑一致性、作用端口的有效性和规则集的正确性，一般的网络系统管理员难以胜任，加之一旦出现新的协议，管理员就得加上更多的规则去限制，这往往会带来很多错误。

（3）攻击者可“假冒”地址，黑客可以在网络上伪造假的路由信息欺骗防火墙。

（4）由于路由器的主要功能是为网络访问提供动态的、灵活的路由，而防火墙则要对访问行为实施静态的、固定的控制，这是一对难以调和的矛盾，防火墙的规则设置会大大降低路由器的性能。

6.3.2 第二代防火墙：用户化的防火墙

1. 用户化防火墙的特点

(1) 将过滤功能从路由器中独立出来，并加上审计和告警功能。

(2) 针对用户需求，提供模块化的软件包。

(3) 软件可通过网络发送，用户可自己动手构造防火墙。

(4) 与第一代防火墙相比，安全性提高而价格降低了。

由于是纯软件产品，第二代防火墙产品无论在实现还是在维护上都对系统管理员提出了相当复杂的要求。

2. 用户化防火墙的不足

(1) 配置和维护过程复杂、费时。

(2) 对用户的技术要求高。

(3) 全软件实现、安全性和处理速度均有局限。

(4) 实践表明，使用中出现差错的情况很多。

6.3.3 第三代防火墙：建立在通用操作系统上的防火墙

基于软件的防火墙在销售、使用和维护上的问题迫使防火墙开发商很快推出了建立在通用操作系统上的商用防火墙产品，近年来在市场上广泛使用的就是这一代产品。

1. 通用操作系统防火墙的特点

(1) 是批量上市的专用防火墙产品。

(2) 包括分组过滤或借用了路由器的分组过滤功能。

(3) 装有专用的代理系统，监控所有协议的数据和指令。

(4) 保护用户编程空间和用户可配置内核参数的设置。

(5) 安全性和速度大为提高。

第三代防火墙有以纯软件实现的，也有以硬件方式实现的。但随着安全需求的变化和使用时间的推延，仍表现出不少问题。

2. 通用操作系统防火墙的不足

(1) 作为基础的操作系统，其内核往往不为防火墙管理者所知，由于原码的保密，其安全性无从保证。

(2) 大多数防火墙厂商并非通用操作系统的厂商，通用操作系统厂商不会对操作系统的安全性负责。

上述问题在基于 Windows NT 开发的防火墙产品中表现得十分明显。

6.3.4 第四代防火墙：具有安全操作系统的防火墙

这是目前防火墙产品的主要发展趋势。具有安全操作系统的防火墙本身就是一个操作系统，因而在安全性上较第三代防火墙有质的提高。获得安全操作系统的办法有两种：一种是通过许可证方式获得操作系统的源码；另一种是通过固化操作系统内核来提高可靠性。

安全操作系统防火墙的特点：

(1) 防火墙厂商具有操作系统的源代码,并可实现安全内核。

(2) 对安全内核实现加固处理,即去掉不必要的系统特性,加上内核特性,强化安全保护。

(3) 对每个服务器、子系统都作了安全处理,一旦黑客攻破了一个服务器,它将会被隔离在此服务器内,不会对网络的其他部分构成威胁。

(4) 在功能上包括了分组过滤、应用网关、电路级网关,且具有加密与鉴别功能。

(5) 透明性好,易于使用。

上述阶段的划分主要以产品为对象,目的在于对防火墙的发展有一个总体勾画。

6.4 防火墙的分类

如果从防火墙的软、硬件形式来分的话,防火墙可以分为软件防火墙和硬件防火墙两种。如果防火墙根据防范的方式和侧重点的不同来进行分类,可分为三大类:包过滤、状态检测包过滤、应用代理。

6.4.1 软件防火墙

软件防火墙运行于特定的计算机上,它需要用户预先安装好的计算机操作系统的支持,一般来说这台计算机就是整个网络的网关。软件防火墙就像其他的软件产品一样需要先在计算机上安装并做好配置才可以使用。使用这类防火墙,需要用户对所工作的操作系统平台比较熟悉。

个人防火墙是软件防火墙中比较常见的一种,可为个人计算机提供简单的防火墙功能。目前常用的个人防火墙有 Norton Personal Firewall、天网个人防火墙、瑞星个人防火墙等。个人防火墙是安装在个人 PC 上,而不是放置在网络边界,因此,个人防火墙关心的不是一个网络到另外一个网络的安全,而是单个主机和与之相连接的主机或网络之间的安全。

个人防火墙使用方便,配置简单,但也具有一定的局限性,其应用范围较小,且只支持 Windows 系统,功能相对来说要弱很多,并且安全性和并发连接处理能力较差。

作为网络防火墙的软件防火墙具有比个人防火墙更强的控制功能和更高的性能。不仅支持 Windows 系统,并且多数都支持 UNIX 或 Linux 系统。如十分著名的 Check Point FireWall、Microsoft ISA Server 等。

软件防火墙与硬件防火墙相比在性能上和抗攻击能力上都比较弱,如果所在的网络环境中,攻击频度不是很高,用软件防火墙就能满足要求。但如果是较大型的网络,就需要硬件防火墙来进行保护了。

6.4.2 包过滤防火墙

包过滤防火墙是用一个软件查看所流经的数据包的包头(header),由此决定整个包的命运。它可能会决定丢弃这个包,可能会接受这个包(让这个包通过),也可能执行其他更复杂的动作。

在 Linux 系统下,包过滤功能是内建于核心的(作为一个核心模块,或者直接内建),同时还有一些可以运用于数据包之上的技巧,不过最常用的依然是查看包头以决定包的命运。

包过滤是一种内置于 Linux 内核路由功能之上的防火墙类型，其防火墙工作在网络层。包过滤防火墙的工作层次如图 6.4 所示。

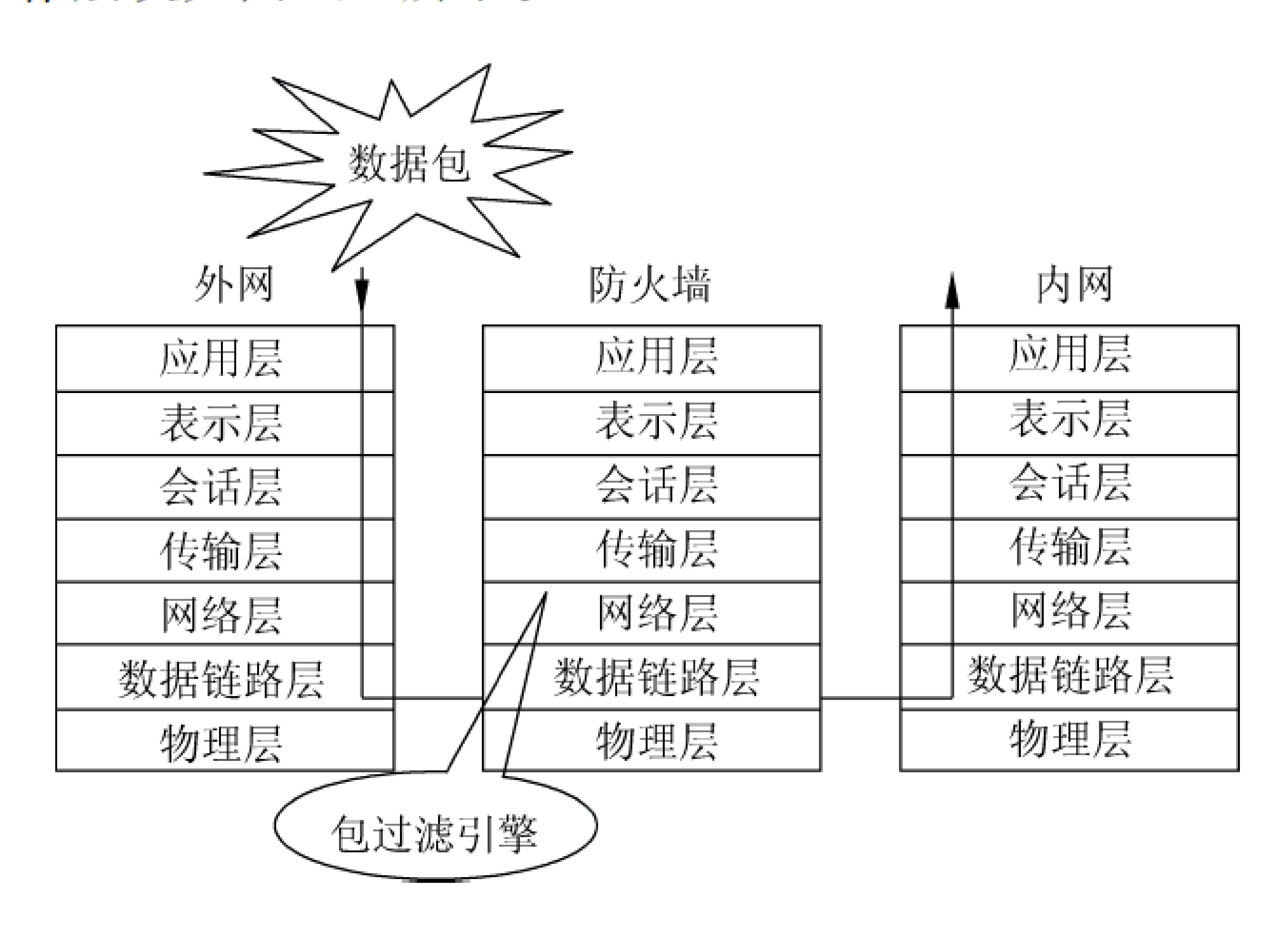


图 6.4　包过滤防火墙的工作层次

1. 工作原理

包过滤防火墙的工作原理可以分为以下几个方面。

(1) 使用过滤器。数据包过滤用在内部主机和外部主机之间，过滤系统是一台路由器或是一台主机。过滤系统根据过滤规则来决定是否让数据包通过。用于过滤数据包的路由器被称为过滤路由器。

数据包过滤是通过对数据包的 IP 头和 TCP 头或 UDP 头的检查来实现的，在 TCP/IP 中，存在着一些标准的服务端口号，例如，HTTP 的端口号为 80。通过屏蔽特定的端口可以禁止特定的服务。包过滤系统可以阻塞内部主机和外部主机或另外一个网络之间的连接，例如，可以阻塞一些被视为是有敌意的或不可信的主机或网络连接到内部网络中。

(2) 过滤器的实现。数据包过滤一般使用过滤路由器来实现，这种路由器与普通的路由器有所不同。普通的路由器只检查数据包的目标地址，并选择一个达到目的地址的最佳路径。它处理数据包是以目标地址为基础的，存在着两种可能性：若路由器可以找到一个路径到达目标地址则发送出去；若路由器不知道如何发送数据包则通知数据包的发送者“数据包不可达”。

过滤路由器会更加仔细地检查数据包，除了决定是否有到达目标地址的路径外，还要决定是否应该发送数据包。“应该与否”是由路由器的过滤策略决定并强行执行的。

(3) 包过滤器操作的基本过程，如图 6.5 所示。

① 包过滤规则必须被包过滤设备端口存储在安全策略设置里。

② 当包到达端口时，对包报头进行语法分析。大多数包过滤设备只检查 IP、TCP 或 UDP 报头中的字段。

③ 包过滤规则以特殊的方式存储。应用于包的规则的顺序与包过滤器规则存储顺序必须相同。

④ 若一条规则阻止包传输或接收，则此包便不符合条件，并被丢弃。

⑤ 若一条规则允许包传输或接收，则此包便符合条件，可以被继续处理。

⑥ 符合条件的包将检查路由信息并被转发出去。

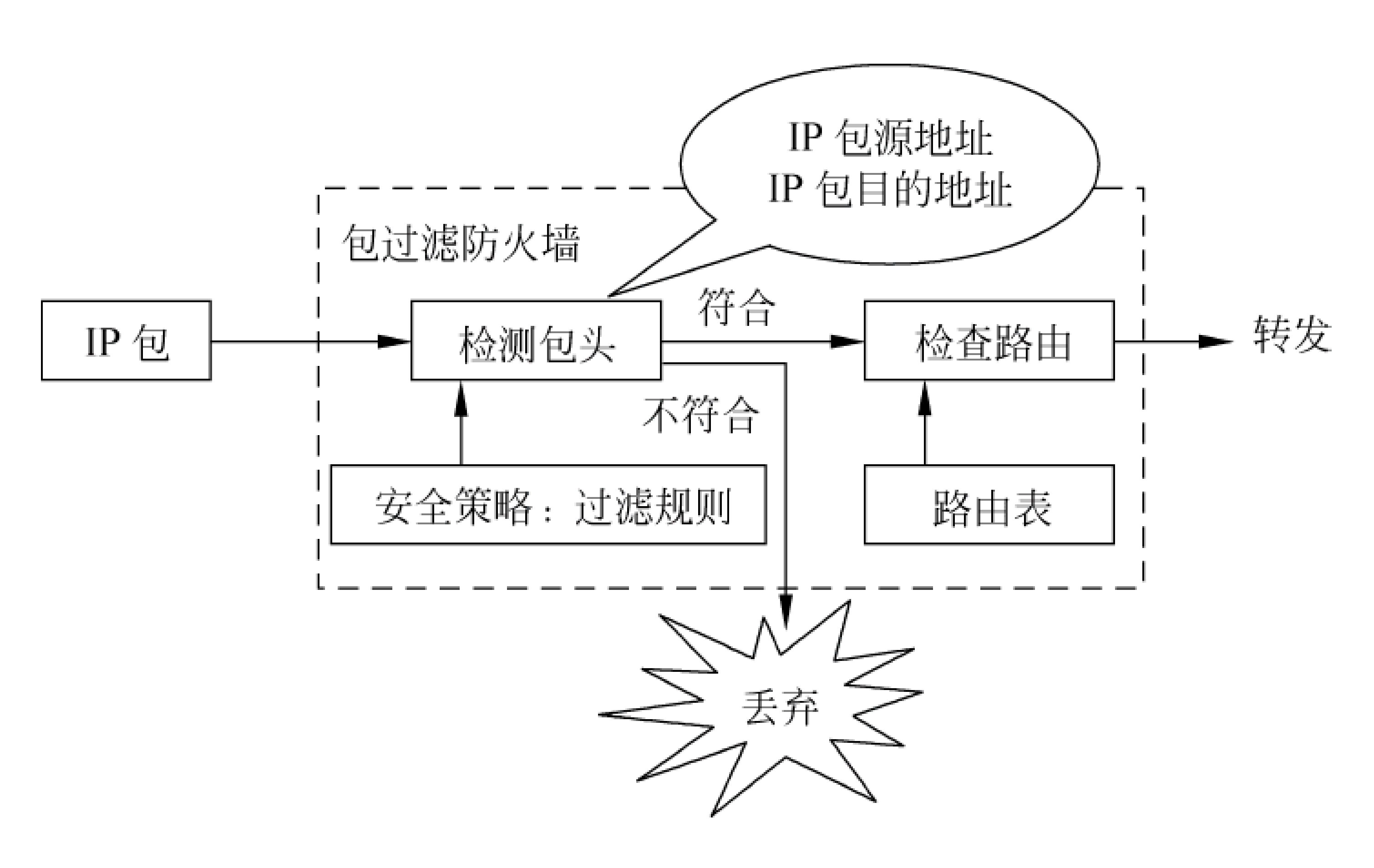


图 6.5　包过滤器操作过程

2. 包过滤技术的优缺点

1）优点

对于一个小型的、不太复杂的站点，包过滤比较容易实现。因为过滤路由器工作在 IP 层和 TCP 层，所以处理包的速度比代理服务器快。

过滤路由器为用户提供了一种透明的服务，用户不需要改变客户端的任何应用程序，也不需要用户学习任何新的东西。因为过滤路由器工作在 IP 层和 TCP 层，而 IP 层和 TCP 层与应用层的问题毫不相关。所以，过滤路由器有时也被称为“包过滤网关”或“透明网关”。之所以被称为网关，是因为包过滤路由器和传统路由器不同，它涉及了传输层。过滤路由器在价格上一般比代理服务器便宜。

2）缺点

一些包过滤网关不支持有效的用户认证。同时规则表很快会变得很大而且复杂，规则很难测试。随着表的增大和复杂性的增加，规则结构出现漏洞的可能性也会增加。

这种防火墙最大的缺陷是它依赖一个单一的部件来保护系统。如果这个部件出现了问题，会使得网络大门敞开，而用户甚至可能还不知道。

在一般情况下，如果外部用户被允许访问内部主机，则它就可以访问内部网上的任何主机。包过滤防火墙只能阻止一种类型的 IP 欺骗，即外部主机伪装内部主机的 IP，对于外部主机伪装外部主机的 IP 欺骗却不可能阻止，而且它不能防止 DNS 欺骗。

虽然，包过滤防火墙有如上所述的缺点，但是在管理良好的小规模网络上，它能够正常地发挥作用。一般情况下，人们不单独使用包过滤网关，而是将它和其他设备（如堡垒主机等）联合使用。

6.4.3　状态检测防火墙

状态检测防火墙又称动态包过滤，是传统包过滤上的功能扩展。状态检测防火墙在网络层有一个检查引擎截获数据包并抽取出与应用层状态有关的信息，并以此为依据决定对该连接是接受还是拒绝。这种技术提供了高度安全的解决方案，同时具有较好的适应性和扩展性。状态检测防火墙一般也包括一些代理级的服务，它们提供附加的对特定应用程序数据内容的支持。状态检测技术最适合提供对 UDP 协议的有限支持。它将所有通过防火

墙的UDP分组均视为一个虚连接,当反向应答分组送达时,就认为一个虚拟连接已经建立。状态检测防火墙克服了包过滤防火墙和应用代理服务器的局限性,不仅仅检测to和from的地址,而且不要求每个访问的应用都有代理。

状态检测防火墙工作于传输层,与包过滤防火墙相比,状态检测防火墙判断允许还是禁止数据流的依据也是源IP地址、目的IP地址、源端口、目的端口和通信协议等。与包过滤防火墙不同的是,状态检测防火墙是基于会话信息做出决策的,而不是包的信息。状态检测防火墙摒弃了包过滤防火墙仅考察数据包的IP地址等几个参数,而不关心数据包连接状态变化的缺点,在防火墙的核心部分建立状态连接表,并将进出网络的数据当成一个个的会话,利用状态表跟踪每一个会话状态。状态监测对每一个包的检查不仅根据规则表,更考虑了数据包是否符合会话所处的状态,因此提供了完整的对传输层的控制能力。

状态检测包过滤器操作的基本过程,如图6.6所示。

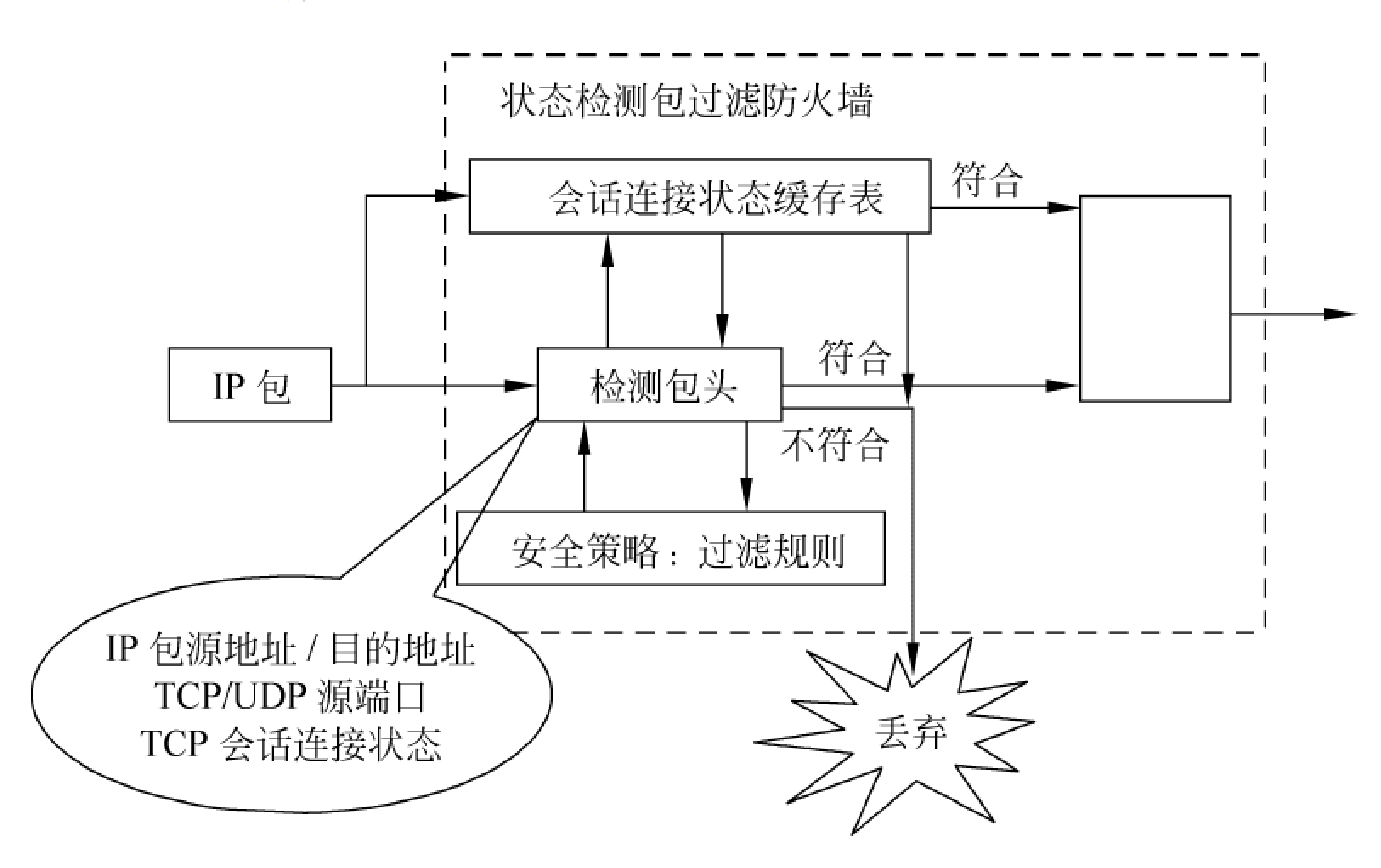


图6.6　状态检测防火墙的工作原理

(1)包过滤规则必须被存储在安全策略设置里。

(2)当包到达端口时,对包报头进行语法分析。同时在会话连接状态缓存表中保持一个状态。

(3)数据包还要和会话连接状态缓存表中的会话所处的状态进行对比,符合规则的才算检测通过。

(4)若一条规则阻止包传输或接收,则此包便不符合条件,并被丢弃。

(5)若一条规则允许包传输或接收,则此包便符合条件,可以被继续处理。

(6)符合条件的包将检查路由信息并被转发出去。

6.4.4　应用代理网关防火墙

应用代理网关防火墙彻底隔断内网与外网的直接通信,内网用户对外网的访问变成防火墙对外网的访问,然后再由防火墙转发给内网用户。所有通信都必须经应用层代理软件转发,访问者任何时候都不能与服务器建立直接的TCP连接,应用层的协议会话过程必须符合代理的安全策略要求。代理网关防火墙工作在应用层,如图6.7所示。

应用代理网关的优点是可以检查应用层、传输层和网络层的协议特征,对数据包的检测

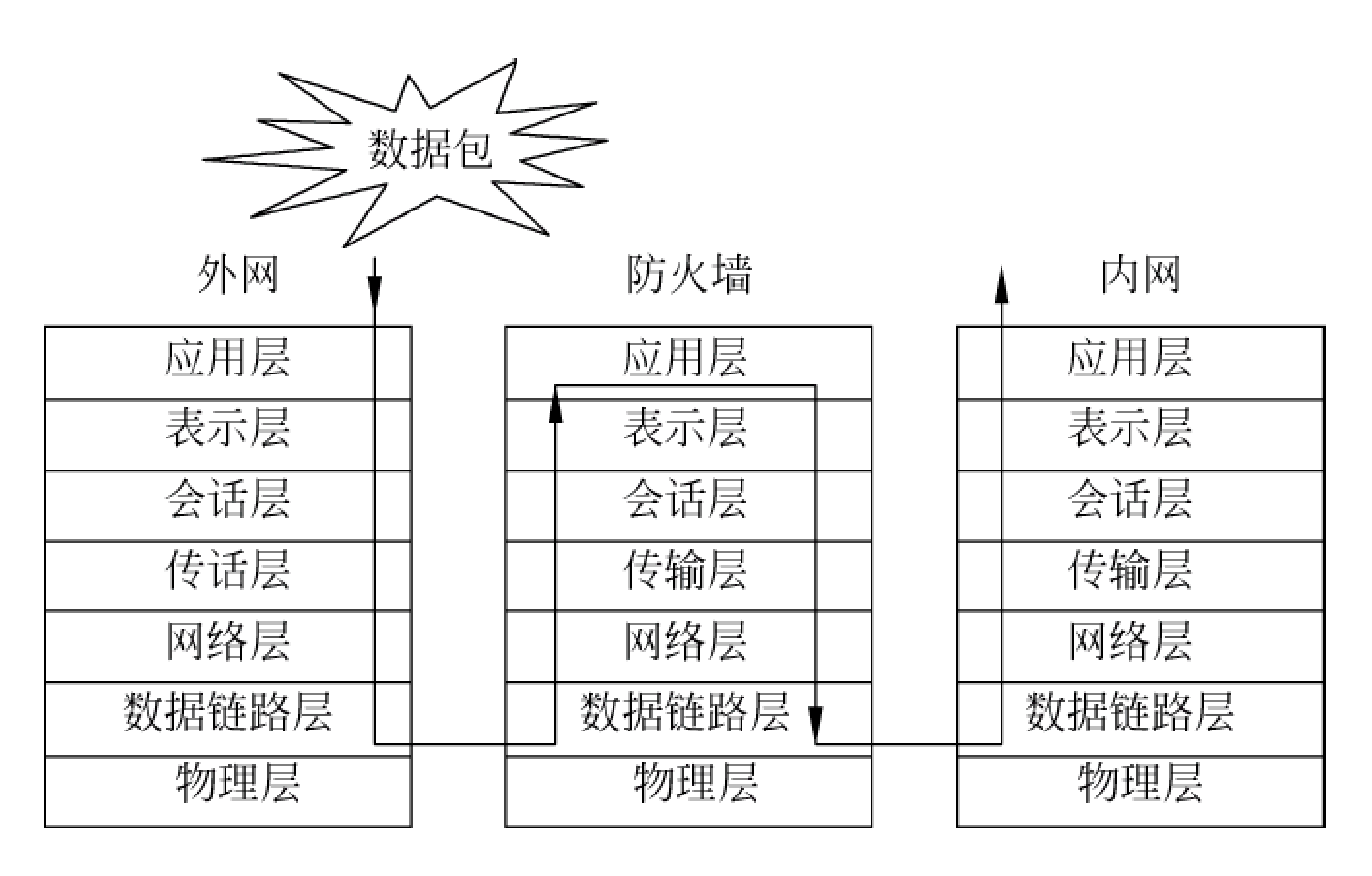


图 6.7　应用代理网关防火墙的工作层次

能力比较强。

应用代理网关的缺点主要有：

（1）难于配置。由于每个应用都要求单独的代理进程，这就要求网管能理解每项应用协议的弱点，并能合理地配置安全策略，由于配置烦琐，难于理解，容易出现配置失误，最终影响内网的安全防范能力。

（2）处理速度非常慢。断掉所有的连接，由防火墙重新建立连接，理论上可以使应用代理防火墙具有极高的安全性。但是实际应用中并不可行，因为对于内网的每个 Web 访问请求，应用代理都需要开一个单独的代理进程，它要保护内网的 Web 服务器、数据库服务器、文件服务器、邮件服务器，及业务程序等，就需要建立一个个的服务代理，以处理客户端的访问请求。这样，应用代理的处理延迟会很大，内网用户的正常 Web 访问不能及时得到响应。

总之，应用代理防火墙不能支持大规模的并发连接，在对速度敏感的行业使用这类防火墙时简直是灾难。另外，防火墙核心要求预先内置一些已知应用程序的代理，使得一些新出现的应用在代理防火墙内被无情地阻断，不能很好地支持新应用。

在 IT 领域中，新应用、新技术、新协议层出不穷，代理防火墙很难适应这种局面。因此，在一些重要的领域和行业的核心业务应用中，代理防火墙正被逐渐疏远。

但是，自适应代理技术的出现让应用代理防火墙技术出现了新的转机，它结合了代理防火墙的安全性和包过滤防火墙的高速度等优点，在不损失安全性的基础上将代理防火墙的性能提高了 10 倍。

6.5　防火墙硬件平台的发展

6.5.1　X86 平台

X86 是一个 Intel 通用计算机系列的标准编号缩写，也标识一套通用的计算机指令集合，X 与处理器没有任何关系，它是一个对所有 X86 系统的简单的通配符定义，例如 386、586、奔腾。由于早期 Intel 的 CPU 编号都是如 8086、80286 来编号，整个系列的 CPU 都是指令兼容的，所以都用 X86 来标识所使用的指令集合，如今的奔腾、赛扬系列都是支持 X86 指令系统的，所以都属于 X86 家族。

X86 指令集是美国 Intel 公司为其第一块 16 位 CPU(i8086)专门开发的。美国 IBM 公司 1981 年推出的世界第一台 PC 中的 CPU 使用的也是 X86 指令,同时计算机中为提高浮点数据处理能力而增加的 X87 芯片系列数学协处理器则另外使用 X87 指令,以后就将 X86 指令集和 X87 指令集统称为 X86 指令集。虽然随着 CPU 技术的不断发展,Intel 陆续研制出更新型的 i80386、i80486 直到今天的 Pentium 4(以下简为 P4)系列,但为了保证计算机能继续运行以往开发的各类应用程序以保护和继承丰富的软件资源,Intel 公司所生产的所有 CPU 仍然继续使用 X86 指令集,它的 CPU 仍属于 X86 系列。

另外除 Intel 公司之外,AMD 和 Cyrix 等厂家也相继生产出能使用 X86 指令集的 CPU,由于这些 CPU 能运行所有的为 Intel CPU 所开发的各种软件,计算机业内人士就将这些 CPU 列为 Intel 的 CPU 兼容产品。由于 Intel X86 系列及其兼容 CPU 都使用 X86 指令集,所以就形成了今天庞大的 X86 系列及兼容 CPU 阵容。

最初的硬件防火墙都是基于 X86 架构的。X86 架构采用通用 CPU 和 PCI 总线接口,具有很高的灵活性和可扩展性,过去一直是防火墙开发的主要平台。其具有开发、设计门槛低,技术成熟等优点,曾经以其高灵活性和扩展性在百兆防火墙上获得过巨大的成功。但是,缺陷也是显而易见的,由于 X86 架构的硬件并非为了网络数据传输而设计,它对数据包的转发性能相对较弱,无法适应日益增长的网络性能要求。

由于国内安全厂商并不掌握 X86 架构的核心技术,其 BIOS 中存在着隐藏的漏洞,有可能影响防火墙的安全可靠性。而且 X86 的产业链条非常复杂,国内厂商在其中能发挥的影响力很有限,不利于国内信息安全产业的长期发展。

6.5.2 ASIC 平台

目前,在集成电路界,ASIC(Application Specific Integrated Circuit,专用集成电路)被认为是一种为专门目的而设计的集成电路,是指应特定用户要求和特定电子系统的需要而设计、制造的集成电路。ASIC 的特点是面向特定用户的需求,ASIC 在批量生产时与通用集成电路相比具有体积更小、功耗更低、可靠性提高、性能提高、保密性增强、成本降低等优点。

ASIC 分为全定制和半定制。全定制设计需要设计者完成所有电路的设计,因此需要大量人力物力,灵活性好但开发效率低下。如果设计较为理想,全定制能够比半定制的 ASIC 芯片运行速度更快。半定制使用库里的标准逻辑单元,设计时可以从标准逻辑单元库中选择 SSI(门电路)、MSI(如加法器、比较器等)、数据通路(如 ALU、存储器、总线等)、存储器甚至系统级模块(如乘法器、微控制器等)和 IP 核,这些逻辑单元已经布局完毕,而且设计得较为可靠,设计者可以较方便地完成系统设计。

相比之下,ASIC 防火墙通过专门设计的 ASIC 芯片逻辑进行硬件加速处理。ASIC 通过把指令或计算逻辑固化到芯片中,获得了很高的处理能力,因而明显提升了防火墙的性能。新一代的高可编程 ASIC 采用了更灵活的设计,能够通过软件改变应用逻辑,具有更广泛的适应能力。但是,ASIC 的缺点也同样明显,它的灵活性和扩展性不够,开发费用高,开发周期太长,一般耗时接近 2 年。

虽然研发成本较高,灵活性受限制,无法支持太多的功能,但其性能具有先天的优势,非常适合应用于模式简单、对吞吐量和时延指标要求较高的电信级大流量的处理。目前,

NetScreen 在 ASIC 防火墙领域占有优势地位，而我国的首信也推出了我国基于自主技术的 ASIC 千兆防火墙产品。

6.5.3 NP 平台

NP(Network Processor，网络处理器)。根据国际网络处理器会议的定义：网络处理器是一种可编程器件，它特定地应用于通信领域的各种任务，比如包处理、协议分析、路由查找、防火墙、QoS 等。

网络处理器器件内部通常由若干个微码处理器和若干硬件协处理器组成，且多个微码处理器在 NP 内部并行处理，通过预先编制的微码来控制处理流程。对于某些复杂的标准操作，如内存操作、路由表查找算法、QoS 的拥塞控制算法、流量调度算法等，则采用硬件协处理器来进一步提高处理性能，从而实现了业务灵活性和高性能的有机结合。

目前 NP 主要用于网络骨干设备和网络接入设备，用来开发从网络第 2 层到第 7 层的各种服务和应用。目前，采用 NP 处理分组交换的厂家，既有第一梯队的网络公司，如思科、北电和朗讯等，也有不少后起之秀，如华为、中兴、港湾等。

哪种 NP 技术更适合防火墙，我们不难了解，由于各厂商所专注的 NP 技术领域不同，决定了 NP 产品之间的差异。目前，国内多数安全厂商在 NP 技术上大都选择了 IBM 或 Intel 的 NP 技术。其实，具体选用哪种 NP 技术开发防火墙，因素有很多，包括所选 NP 技术的性能和成熟度、提供 NP 技术的厂商实力和重视程度，以及 NP 技术厂商可提供的支持力度及价格。

IBM 研发的 Power NP 系列芯片不仅支持多线程，且每个线程都有充足的指令空间，在一个线程里完成防火墙功能绰绰有余。其系列产品中，以 NP4GS3 为代表，该芯片最高端口速率可达 OC-48(2488.32Mb/s)，并具有 4.5Mb/s 的报文处理能力和最大 4GB 的端口容量，并且，其拥有 IBM 创新的带宽分配技术(BAT)，是进行下一代系统设计的强大部件。而且，IBM 还为开发者提供了软件架构的解决方案和仿真平台，大大缩短了开发难度和周期。目前，已经有不少厂家采用 IBM 的芯片开发高端防火墙产品，如联想网御于 2003 年 10 月推出了国内第一款基于 NP 技术的千兆线速防火墙；2005 年，在解决了多项基于多 NP 协同工作的技术难题的基础上，联想网御成功推出了万兆级的超性能防火墙。

Intel 推出的 IXP2000 系列芯片支持微码开发，在性能上有了长足的提高，如 IXP2400 理论上最多可支持 2.5Gb/s 的应用，IXP2800 则支持 10Gb/s 以上的应用。其 SDK 开发包一般功能十分齐全，模块化很好，便于开发人员控制。不足的是，IXP2400 每个微引擎仅能存储 32×4Kb 的指令，比较适合开发路由器和交换机这类产品；IXP2800 每个微引擎能存储 32×8Kb 位的指令，基本可以满足防火墙功能开发的需要，但是，由于其性能提高带来了产品设计与应用复杂度的成倍提高，造成价格十分昂贵。此外，该系列产品的硬件查表功能比较弱，这对于防火墙这类需要大量查表操作的设备来讲，是致命的弱点。

随着新一代网络的继续发展，NP 将更加倚重线速、智能化的包处理技术，而不仅仅是简单的基本性能，NP 技术的发展将直接影响到 NP 防火墙的发展。据业内专家调查分析，NP 技术将向着更高的性能、更多功能支持、多种技术并存和标准化等特征发展，基于 NP 的防火墙产品将随着 NP 的发展大步前行。

五年来，网络的传输速度每年翻一番，几年前的主干网速度是 155Mb/s，现在已经到了

10Gb/s,两到三年内又会提高到 40Gb/s,网络处理器也必须满足这种变化。NP 性能的提高,将直接推动防火墙性能的提高。

随着网络处理器在更多领域中的应用,网络处理器必须具有更多的功能支持,如深度内容处理和 IPv6 协议识别,以能适应防火墙等安全设备的需求。

NP 不是万能的,它并不会完全取代通用处理器和 ASIC 在网络设备中的应用。在对处理性能需求很高的高端设备中,ASIC 仍然具有很强的生命力,可以预见的是,在数据层面、控制层面和管理层,通用处理器、NP 和 ASIC 将各司其职,共同为防火墙应用提供灵活的服务。

总之,防火墙技术与 NP 技术开始紧密地联系在一起,NP 技术的变革将推动防火墙技术向着更高性能、更多功能以及标准化的方向发展。

6.6 防火墙关键技术

6.6.1 访问控制

访问控制是策略和机制的集合,它允许对限定资源的授权访问。它也可保护资源,防止那些无权访问资源的用户的恶意访问或偶然访问。然而,它无法阻止被授权组织的故意破坏。

按用户身份及其所归属的某预定义组来限制用户对某些信息项的访问,或限制对某些控制功能的使用。访问控制通常用于系统管理员控制用户对服务器、目录、文件等网络资源的访问。访问控制机制决定用户及代表一定用户利益的程序能做什么,以及做到什么程度。

访问控制是信息安全保障机制的核心内容,它是实现数据保密性和完整性机制的主要手段。它是对信息系统资源进行保护的重要措施,也是计算机系统中最重要和最基础的安全机制。访问控制包括 3 个要素,即主体、客体和控制策略。

(1) 主体(subject):是可以对其他实体施加动作的主动实体,有时也称为用户或访问者(被授权使用计算机的人员)。主体的含义是广泛的,可以是用户所在的组织、用户本身,也可以是用户使用的计算机终端、卡机、手持终端(无线)等,甚至可以是应用服务程序或进程。

(2) 客体(object):是接受其他实体访问的被动实体。客体的概念也很广泛,凡是可以被操作的信息、资源、对象都可以认为是客体。在信息社会中,客体可以是信息、文件、记录等的集合体,也可以是网络上的硬件设施、无线通信中的终端,甚至一个客体可以包含另外一个客体。

(3) 控制策略:是主体对客体的操作行为集合约束条件集。简单讲,控制策略是主体对客体的访问规则集,这个规则集直接定义了主体对客体的作用行为和客体对主体的条件约束。访问策略体现了一种授权行为,也就是客体对主体的权限允许,这种允许不超越规则集。

防火墙上应用的访问控制技术是网络安全防范和保护的主要核心策略,它的主要任务是保证网络资源不被非法使用和访问。访问控制规定了主体对客体访问的限制,并在身份识别的基础上,根据身份对提出资源访问的请求加以控制。网络访问控制技术是对网络信

息系统资源进行保护的重要措施，也是计算机系统中最重要和最基础的安全机制。

6.6.2 网络地址转换

网络地址转换(NAT)被广泛应用于各种类型 Internet 接入方式和各种类型的网络中。原因很简单，NAT 不仅完美地解决了 lP 地址不足的问题，而且还能够有效地避免来自网络外部的攻击，隐藏并保护网络内部的计算机。

虽然 NAT 可以借助于某些代理服务器来实现，但考虑到运算成本和网络性能，很多时候都是在路由器和防火墙上来实现的。

随着接入 Internet 的计算机数量的不断猛增，IP 地址资源也就愈加显得捉襟见肘。事实上，除了中国教育网(CERNET)外，一般用户几乎申请不到整段的 C 类 IP 地址。在其他 ISP 那里，即使是拥有几百台计算机的大型局域网用户，当他们申请 IP 地址时，所分配的地址也不过只有几个或十几个 IP 地址。显然，这样少的 IP 地址根本无法满足网络用户的需求，于是也就产生了 NAT 技术。

借助于 NAT，私有(保留)地址的内部网络通过防火墙发送数据包时，私有地址被转换成合法的 IP 地址，一个局域网只需使用少量 IP 地址(甚至是 1 个)即可实现私有地址网络内所有计算机与 Internet 的通信需求。

NAT 将自动修改 IP 报文头的源 IP 地址和目的 IP 地址，IP 地址校验则在 NAT 处理过程中自动完成。有些应用程序将源 IP 地址嵌入到 IP 报文的数据部分中，所以还需要同时对报文进行修改，以匹配 IP 头中已经修改过的源 IP 地址。否则，在报文数据都分别嵌入 IP 地址的应用程序就不能正常工作。

NAT 的实现方式有以下三种，即静态转换(static nat)、动态转换(dynamic nat) 和端口地址转换(Port Address Translation，PAT)。

(1) 静态转换是指将内部网络的私有 IP 地址转换为公有 IP 地址，IP 地址对是一对一的，是一成不变的，某个私有 IP 地址只转换为某个公有 IP 地址。借助于静态转换，可以实现外部网络对内部网络中某些特定设备(如服务器)的访问。

(2) 动态转换是指将内部网络的私有 IP 地址转换为公用 IP 地址时，IP 地址对不是确定的，而是随机的，所有被授权访问 Internet 的私有 IP 地址可随机转换为任何指定的合法 IP 地址。也就是说，只要指定哪些内部地址可以进行转换，以及用哪些合法地址作为外部地址时，就可以进行动态转换。动态转换可以使用多个合法外部地址集。当 ISP 提供的合法 IP 地址略少于网络内部的计算机数量时。可以采用动态转换的方式。

(3) 端口地址转换是指改变外出数据包的源端口并进行端口转换。采用端口地址转换方式时，内部网络的所有主机均可共享一个合法外部 IP 地址实现对 Internet 的访问，从而可以最大限度地节约 IP 地址资源。同时，又可隐藏网络内部的所有主机，有效避免来自 Internet 的攻击。因此，目前网络中应用最多的就是端口地址转换方式。

在配置网络地址转换的过程之前，首先必须搞清楚内部接口和外部接口，以及在哪个外部接口上启用 NAT。通常情况下，连接到用户内部网络的接口是 NAT 内部接口，而连接到外部网络(如 Internet)的接口是 NAT 外部接口。在网络中的具体配置如图 6.8 所示。

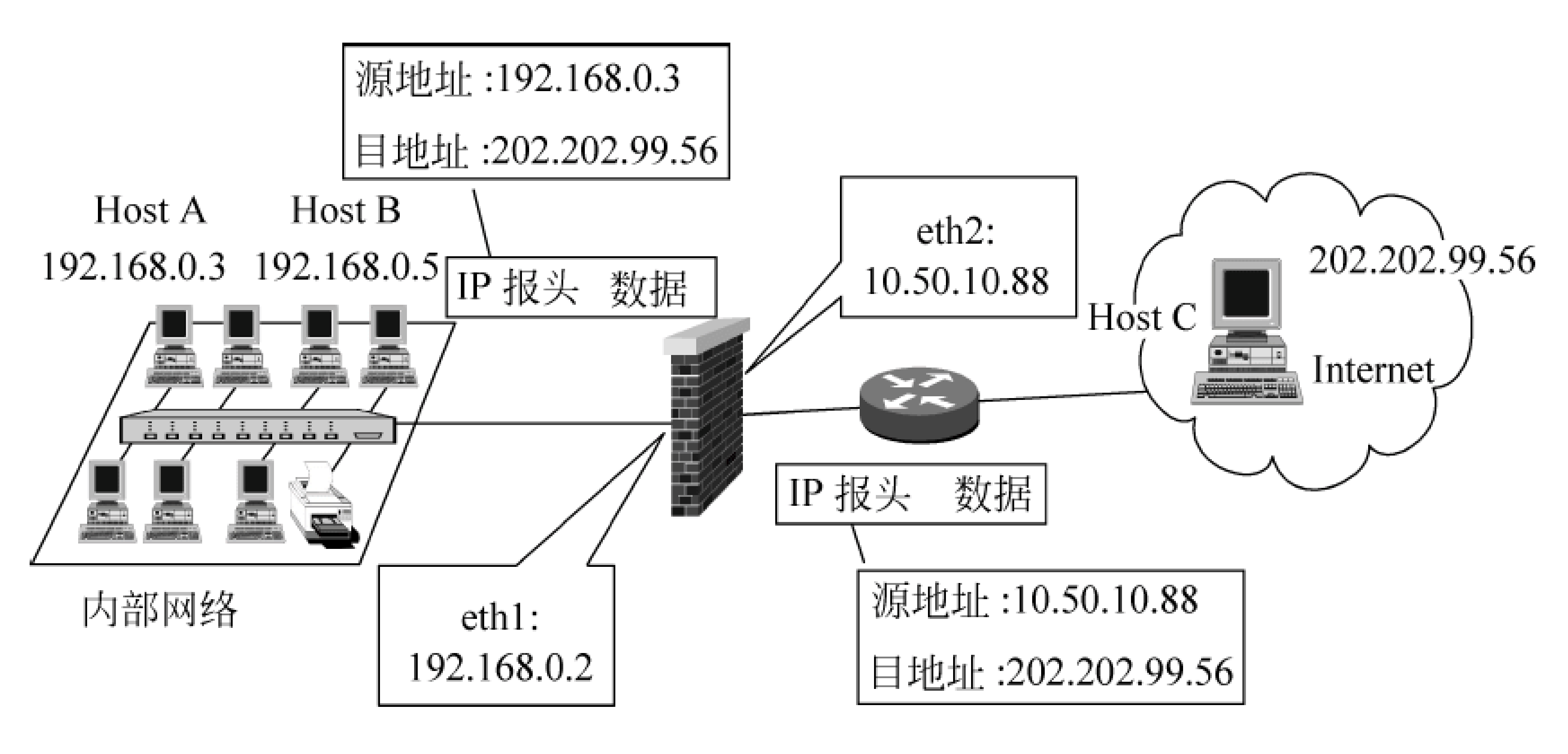


图 6.8 NAT 的配置

6.6.3 虚拟专用网

顾名思义,虚拟专用网(Virtual Private Network,VPN)是虚拟出来的企业内部专线网络。它可以通过特殊的加密的通信协议在 Internet 上的位于不同地方的两个或多个企业内部网之间建立一条专有的通信线路,就好比是架设了一条专线一样,但是它并不需要真正地去铺设光缆之类的物理线路。在网络中的实现如图 6.9 所示。这就好比去电信局申请到了专线,但是不用给铺设线路的费用,也不用购买路由器等硬件设备。VPN 技术原是路由器具有的重要技术之一,目前在交换机、防火墙设备或 Windows 2003 等软件里也都支持 VPN 功能,一句话,VPN 的核心就是在利用公共网络建立虚拟私有网(在第 8 章中会详细说明)。

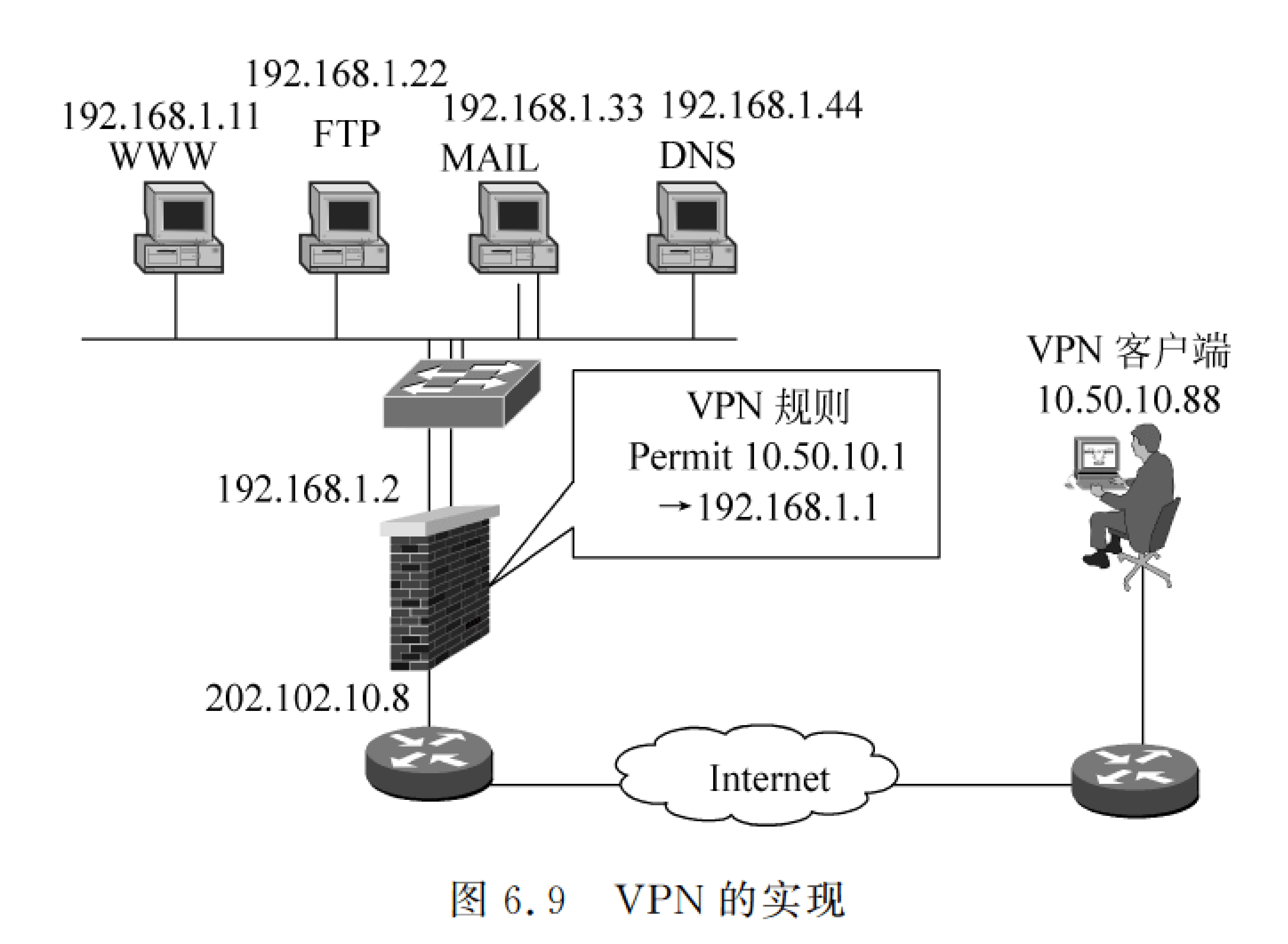


图 6.9 VPN 的实现

课 后 习 题

选择题

1. 一个数据包过滤系统被设计成允许你要求服务的数据包进入,而过滤掉不必要的服务。这属于(　　)基本原则。

A. 最小特权　　B. 阻塞点　　C. 失效保护状态　　D. 防御多样化

2. 针对数据包过滤和应用网关技术存在的缺点而引入的防火墙技术，这是(　　)防火墙的特点。

A. 包过滤型　　B. 应用级网关型

C. 复合型防火墙　　D. 代理服务型

3. 不属于传统防火墙的类型有(　　)。

A. 包过滤　　B. 远程磁盘镜像技术

C. 电路层网关　　D. 应用层网关

4. 在防火墙技术中，内网这一概念通常指的是(　　)。

A. 受信网络　　B. 非受信网络

C. 防火墙内的网络　　D. 互联网

5. Internet 接入控制不能对付以下哪类入侵者？(　　)

A. 伪装者　　B. 违法者

C. 内部用户　　D. 外部用户

填空题

1. 新型防火墙的设计目标是既有(　　)的功能，又能在(　　)进行代理，能从链路层到应用层进行全方位安全处理。

2. 防火墙只对符合安全策略的通信通过，也可以说具有(　　)性。

3. DMZ 是英文 DeMilitarized Zone 的缩写，中文名称为(　　)，也称(　　)。

4. DMZ 在(　　)和(　　)之间构造了一个安全地带。

5. 第一代防火墙是基于(　　)的防火墙，第二代防火墙是(　　)的防火墙，第三代防火墙是(　　)的防火墙，第四代防火墙是(　　)的防火墙。

6. NAT 的实现方式有三种，即(　　)、(　　) 和(　　)。

7. (　　)防火墙彻底隔断内网与外网的直接通信，内网用户对外网的访问变成防火墙对外网的访问，然后再由防火墙转发给内网用户。

简答题

1. 防火墙的主要功能是什么？

2. 防火墙的基本特性有哪些？

3. 防火墙能做什么？

4. DMZ 网络访问控制策略有哪些？

5. 防火墙不能做什么？

6. 防火墙的种类有哪些？

7. 包过滤防火墙的工作原理是什么？

8. 包过滤技术的优缺点有哪些？

9. 防火墙硬件平台有哪些种类？各自的特点是什么？

10. 你所知道的防火墙品牌有哪些？

11. 应用代理防火墙是怎样工作的？

12. 访问控制的功能主要有哪些？

第7章 入侵检测系统

7.1 入侵检测系统是什么

计算机安全的三大中心目标是：保密性、完整性、可用性。人们在实现这些目标的过程中不断进行着探索和研究。其中比较突出的技术有身份认证与识别、访问控制机制、加密技术、防火墙技术等。但是这些技术的一个共同特征就是集中在系统的自身加固和防护上，属于静态的安全防御技术，它对于网络环境下日新月异的攻击手段缺乏主动的反应。针对日益严重的网络安全问题和越来越突出的安全需求，自适应网络安全技术(动态安全技术)和动态安全模型应运而生。

入侵检测作为动态安全技术的核心技术之一，是防火墙的合理补充，帮助系统对付网络攻击，扩展了系统管理员的安全管理能力(包括安全审计、监视、进攻识别和响应)，提高了信息安全基础结构的完整性，是安全防御体系的一个重要组成部分。

入侵检测系统(Intrusion-Detection System，IDS)是一种对网络传输进行即时监视，在发现可疑传输时发出警报或者采取主动反应措施的网络安全设备。它与其他网络安全设备的不同之处在于，IDS是一种积极主动的安全防护技术。IDS最早出现在1980年4月。该年，James P. Anderson为美国空军做了一份题为“Computer Security Threat Monitoring and Surveillance”(计算机安全威胁监控与监视)的技术报告，提出审计记录可用于检测计算机误用行为的思想，在其中他提出了IDS的概念，这可谓是开创了入侵检测的先河。20世纪80年代中期，IDS逐渐发展成为入侵检测专家系统(IDES)。另一位对入侵检测同样起着开创作用的人就是Dorothy E. Denning，他在1987年的一篇论文中提出了实时入侵检测系统模型，此模型成为后来的入侵检测研究和系统原型的基础。1990年，IDS分化为基于网络的IDS和基于主机的IDS。后又出现分布式IDS。目前，IDS发展迅速，已有人宣称IDS可以取代防火墙。

假如防火墙是一幢大楼的保安，那么IDS就是这幢大楼里的监控系统。一旦小偷爬窗进入大楼，或内部人员有越界行为，只有实时监视系统才能发现情况并发出警告，如图7.1所示。

早期的入侵检测系统是基于主机的系统，它是通过监视和分析主机的审计记录来检测入侵的。另外，入侵检测发展史上又一个具有重要意义的里程碑就是NSM(Network Security Monitor，网络安全监视器)的出现，它是由L. Todd Heberlien在1990年提出的。NSM与此前的入侵检测系统相比，其最大的不同在于它并不检查主机系统的审计记录，而是通过监视网络的信息流量来跟踪可疑的入侵行为。从此，入侵检测的研究和开发呈现一股热潮，而且多学科多领域之间知识的交互使得入侵检测的研究异彩纷呈。

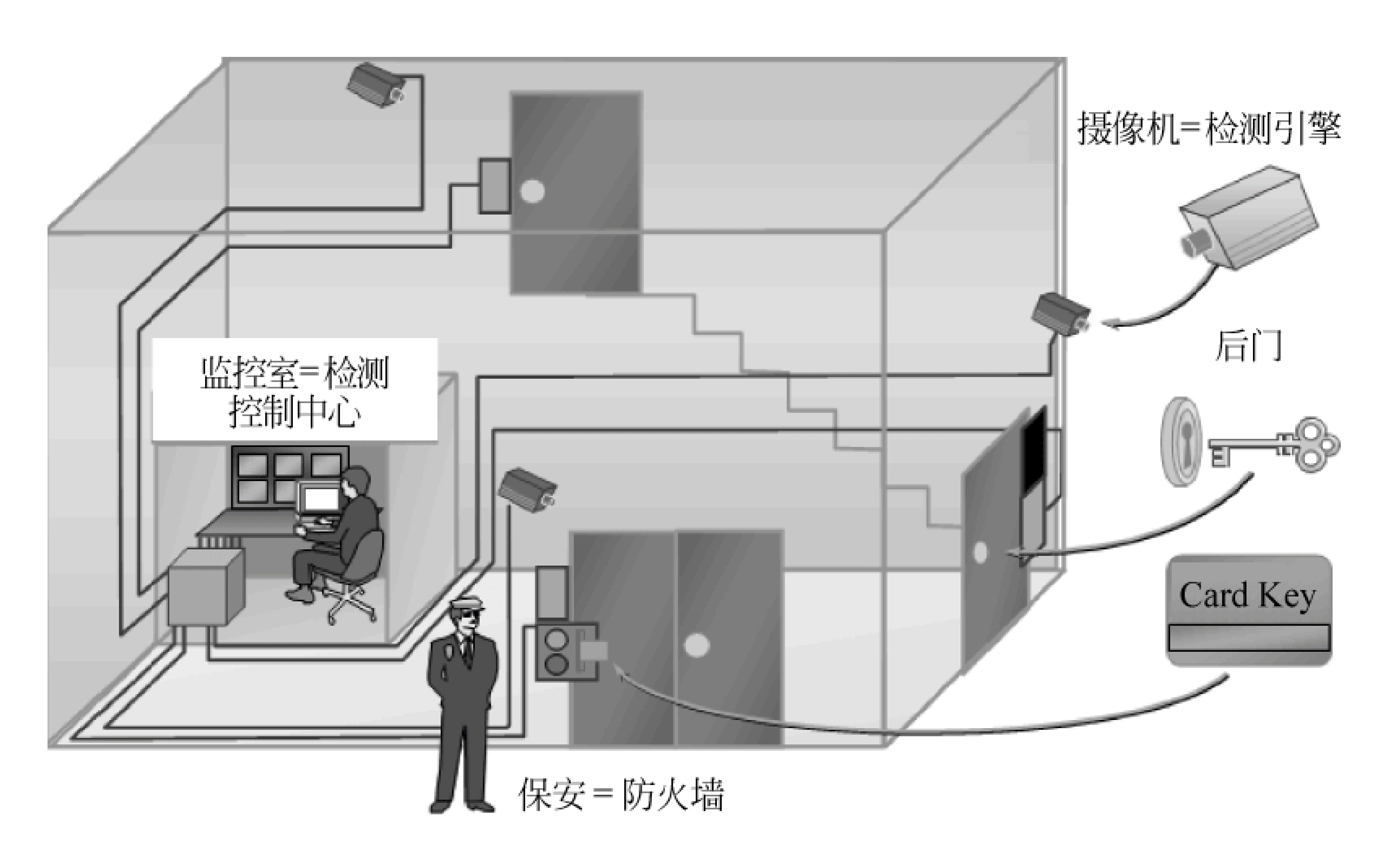


图 7.1　理解入侵检测系统

由于入侵检测系统的市场在近几年中飞速发展，许多公司投入到这一领域中来。Venustech(启明星辰)、Internet Security System(ISS)、思科、赛门铁克等公司都推出了自己的产品。

7.2　入侵检测基本原理

从计算机安全的目标来看，入侵的定义是：企图破坏资源的完整性、保密性、可用性的任何行为，也指违背系统安全策略的任何事件。入侵行为不仅仅是指来自外部的攻击，同时内部用户的未授权行为也是一个重要的方面，有时内部人员滥用他们特权的攻击是系统安全的最大隐患。从入侵策略的角度来看，入侵可分为企图进入、冒充其他合法用户、成功闯入、合法用户的泄露、拒绝服务以及恶意使用等几个方面。

入侵检测就是通过从计算机网络或计算机系统中若干关键点收集信息并对其进行分析，从中发现网络或系统中是否有违反安全策略的行为和遭到攻击的迹象，同时做出响应。从上述的定义可以看出，入侵检测的一般过程是：信息收集、信息(数据)预处理、数据的检测分析、根据安全策略做出响应，如图 7.2 所示。

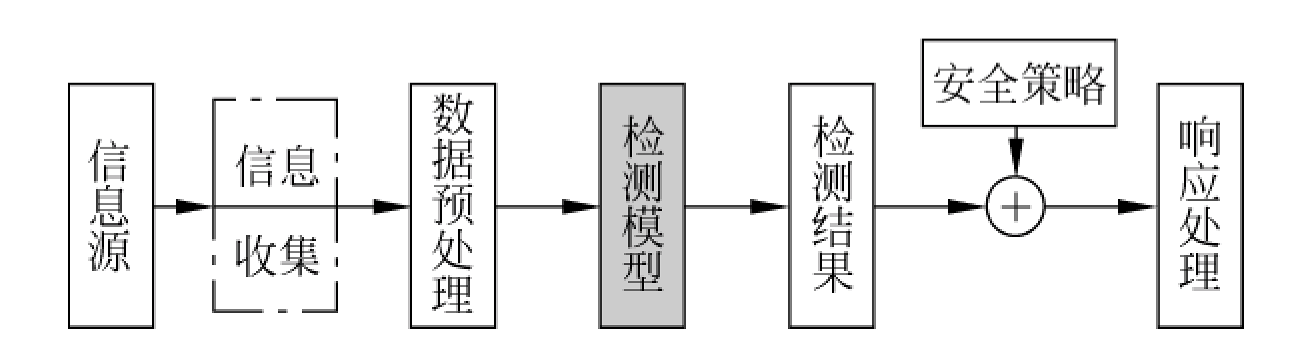


图 7.2　入侵检测的一般过程

其中，信息源是指包含有最原始的入侵行为信息的数据，主要是网络、系统的审计数据或原始的网络数据包。数据预处理是指对收集到的数据进行预处理，将其转化为检测模型所接受的数据格式，也包括对冗余信息的去除，即数据简约。这是入侵检测研究领域的关键，也是难点之一。检测模型是指根据各种检测算法建立起来的检测分析模型，它的输入一般是经过数据预处理后的数据，输出为对数据属性的判断结果，数据属性一般是针对数据中

包含的入侵信息的断言。

检测结果即检测模型输出的结果，由于单一的检测模型的检测率不理想，往往需要利用多个检测模型进行并行分析处理，然后对这些检测结果进行数据融合处理，以达到满意的效果。安全策略是指根据安全需求设置的策略。响应处理主要是指综合安全策略和检测结果所作出的响应过程，包括产生检测报告、通知管理员、断开网络连接或更改防火墙的配置等积极的防御措施。

入侵检测系统就其最基本的形式来讲，可以说是一个分类器，它是根据系统的安全策略来对收集到的事件或状态信息进行分类处理，从而判断出入侵和非入侵的行为的。

一般来说，入侵检测系统在功能结构上是基本一致的，均由数据采集、数据分析以及响应部件等几个功能模块组成，只是具体的入侵检测系统在采集数据、采集数据的类型以及分析数据的方法等方面有所不同而已。但是由于入侵技术手段的不断变化，使得入侵检测系统必须能够维护一些与检测系统的分析技术相关的信息，以使检测系统能够确保检测出对系统具有威胁的恶意事件。

显然，入侵检测系统完善了以前的静态安全防御技术的诸多不足，是对防火墙的合理补充，为计算机网络、系统的安全防护提供了新的解决方案。

7.3 入侵检测系统分类

入侵检测系统作为动态安全防御技术的应用实例，是继防火墙之后的第二道安全防线，它的运用将大大提高系统安全防护水平。入侵检测系统的分类有多种，这里主要介绍两种：一种是根据入侵检测系统的输入数据来源分类；另一种是根据入侵检测系统所采用的技术分类。

7.3.1 按数据来源分类

由于入侵检测是个典型的数据处理过程，因而数据采集是其第一步。同时，针对不同的数据类型，所采用的分析机理也是不一样的。根据入侵检测系统输入数据的来源来看，它可分为基于主机的入侵检测系统和基于网络的入侵检测系统。

1. 基于主机(host-based)的入侵检测系统

基于主机的入侵检测系统(HIDS)通常以系统日志、应用程序日志等审计记录文件作为数据源。它是通过比较这些审计记录文件的记录与攻击签名(attack signature，指用一种特定的方式来表示已知的攻击模式)以发现它们是否匹配。如果匹配，检测系统就向系统管理员发出入侵报警并采取相应的行动。基于主机的 IDS 可以精确地判断入侵事件，并可对入侵事件作出立即反应。它还可针对不同操作系统的特点判断出应用层的入侵事件。

由于审计数据是收集系统用户行为信息的主要方法，因而必须保证系统的审计数据不被修改。但是，当系统遭到攻击时，这些数据很可能被修改。这就要求基于主机的入侵检测系统必须满足一个重要的实时性条件：检测系统必须在攻击者完全控制系统并更改审计数据之前完成对审计数据的分析、产生报警并采取相应的措施。早期的入侵检测系统大多都是基于主机的 IDS，作为入侵检测系统的一大重要类型，它具有明显的优点：

(1) 能够确定攻击是否成功。由于基于主机的 IDS 使用包含有确实已经发生的事件信

息的日志文件作为数据源，因而比基于网络的 IDS 更能准确地判断出攻击是否成功。在这一点上，基于主机的 IDS 可谓是基于网络的 IDS 的完美补充。

(2) 非常适合于加密和交换环境。由于基于网络的 IDS 是以网络数据包作为数据源，因而对于加密环境来讲，它是无能为力的，但对于基于主机的 IDS 就不同了，因为所有的加密数据在到达主机之前必须被解密，这样才能被操作系统所解析。对于交换网络来讲，基于网络的 IDS 在获取网络流量上面临着很大的挑战，但基于主机的 IDS 就没有这方面的限制。

(3) 近乎实时的检测和响应。基于主机的 IDS 不能提供真正的实时响应，但是由于现有的基于主机的 IDS 大多采取的是在日志文件形成的同时获取审计数据信息，因而就为实时的检测和响应提供了可能。

(4) 不需要额外的硬件。基于主机的 IDS 是驻留在现有的网络基础设施之上的，包括文件服务器、Web 服务器和其他共享资源等，这样就减少了基于主机的 IDS 的实施成本。因为不再需要增加新的硬件，所以也就减少了以后维护和管理这些硬件设备的负担。

(5) 可监视特定的系统行为。基于主机的 IDS 可以监视用户和文件的访问活动，这包括文件访问、文件权限的改变、试图建立新的可执行文件和试图访问特权服务等。例如，基于主机的 IDS 可以监视所有的用户登录及注销情况，以及每个用户连接到网络以后的行为。而基于网络的 IDS 就很难做到这一点。基于主机的 IDS 还可以监视通常只有管理员才能实施的行为，因为操作系统记录了任何有关用户账号的添加、删除、更改的情况，一旦发生了更改，基于主机的 IDS 就能检测到这种不适当的更改。基于主机的 IDS 还可以跟踪影响系统日志记录的策略的变化。

(6) 基于主机的 IDS 可以监视关键系统文件和可执行文件的更改。试图对关键的系统文件进行覆盖或试图安装特洛伊木马或后门程序的操作都可被检测出并被终止，而基于网络的 IDS 有时就做不到这一点。

除了上述的优点外，基于主机的 IDS 也存在一些不足：会占用主机的系统资源，增加系统负荷，而且针对不同的操作系统必须开发出不同的应用程序，另外，所需配置的 IDS 数量众多。但是对系统内在的结构没有任何的约束，同时可以利用操作系统本身提供的功能，并结合异常检测分析，更能准确地报告攻击行为。

2. 基于网络的入侵检测系统

基于网络的入侵检测系统(NIDS)以原始的网络数据包作为数据源。它是利用网络适配器来实时地监视并分析通过网络进行传输的所有通信业务的。一旦检测到攻击，IDS 的响应模块通过通知、报警以及中断连接等方式来对攻击行为作出反应。作为入侵检测发展史上的一个里程碑，基于网络的 IDS 是在网络迅速发展、攻击手段日趋复杂的情况下出现的新产物，它以其独特的技术手段在入侵检测的舞台上扮演着不可或缺的角色。较之于基于主机的 IDS，它有着自身明显的优势：

(1) 攻击者转移证据更困难，基于网络的 IDS 使用正在发生的网络通信进行实时攻击的检测，因此攻击者无法转移证据，被检测系统捕获到的数据不仅包括攻击方法，而且包括对识别和指控入侵者十分有用的信息。由于很多黑客对审计日志很了解，因而他们知道怎样更改这些文件以藏匿他们的入侵踪迹，而基于主机的 IDS 往往需要这些原始的未被修改的信息来进行检测，在这一点上，基于网络的 IDS 有着明显的优势。

(2) 实时检测和应答，一旦发生恶意的访问或攻击，基于网络的 IDS 可以随时发现它

们,以便能够更快地作出反应。这种实时性使得系统可以根据预先的设置迅速采取相应的行动,从而将入侵行为对系统的破坏减到最低,而基于主机的 IDS 只有在可疑的日志文件产生后才能判断攻击行为,这时往往对系统的破坏已经产生了。

(3) 能够检测到未成功的攻击企图,有些攻击行为是旨在针对防火墙后面的资源的攻击(防火墙本身可能会拒绝这些攻击企图),利用放置在防火墙外的基于网络的 IDS 就可以检测到这种企图,而基于主机的 IDS 并不能发现未能到达受防火墙保护的主机的攻击企图。通常,这些信息对于评估和改进系统的安全策略是十分重要的。

(4) 操作系统无关性,基于网络的 IDS 并不依赖主机的操作系统作为检测资源,这样就与主机的操作系统无关,而基于主机的系统需要依赖特定的操作系统才能发挥作用。

(5) 较低的成本,基于网络的 IDS 允许部署在一个或多个关键访问点来检查所有经过的网络通信,因此,基于网络的 IDS 系统并不需要在各种各样的主机上进行安装,大大减少了安全和管理的复杂性,这样所需的成本费用也就相对较低。

当然,对于基于网络的 IDS 来讲,同样有着一定的不足:它只能监视通过本网段的活动,并且精确度较差,在交换网络环境中难于配置,防欺骗的能力比较差,对于加密环境它就更是无能为力了。

3. 分布式的入侵检测系统

从以上对基于主机的 IDS 和基于网络的 IDS 的分析可以看出:这两者各自都有着自身独到的优势,而且在某些方面是很好的互补。如果采用这两者结合的入侵检测系统,那将是汲取了各自的长处,又弥补了各自的不足的一种优化设计方案。通常,这样的系统一般为分布式结构,由多个部件组成,它能同时分析来自主机系统的审计数据及来自网络的数据通信流量信息。分布式的 IDS 是目前人们研究的重点,它是一种相对完善的体系结构,为日趋复杂的网络环境下的安全策略的实现提供了最佳的解决对策。

7.3.2 按分析技术分类

从入侵检测的典型实现过程可以看出,数据分析是入侵检测系统的核心,它是能否检测出入侵行为的关键。检测率是人们关注的焦点,不同的分析技术所体现的分析机制也是不一样的,从而对数据分析得到的结果当然也就大不相同,而且不同的分析技术对不同的数据环境的适用性也不一样。根据入侵检测系统所采用的分析技术来看,它可以分为采用异常检测的入侵检测系统和采用误用检测的入侵检测系统。

1. 异常检测(anomaly detection)

异常检测也被称为基于行为的检测。其基本前提是:假定所有的入侵行为都是异常的,即入侵行为是异常行为的子集。原理是:首先建立系统或用户的"正常"行为特征轮廓,通过比较当前的系统或用户的行为是否偏离正常的行为特征轮廓来判断是否发生了入侵行为,而不是依赖于具体行为是否出现来进行检测的。从这个意义上来讲,异常检测是一种间接的方法。图 7.3 是典型的异常检测系统示意图。

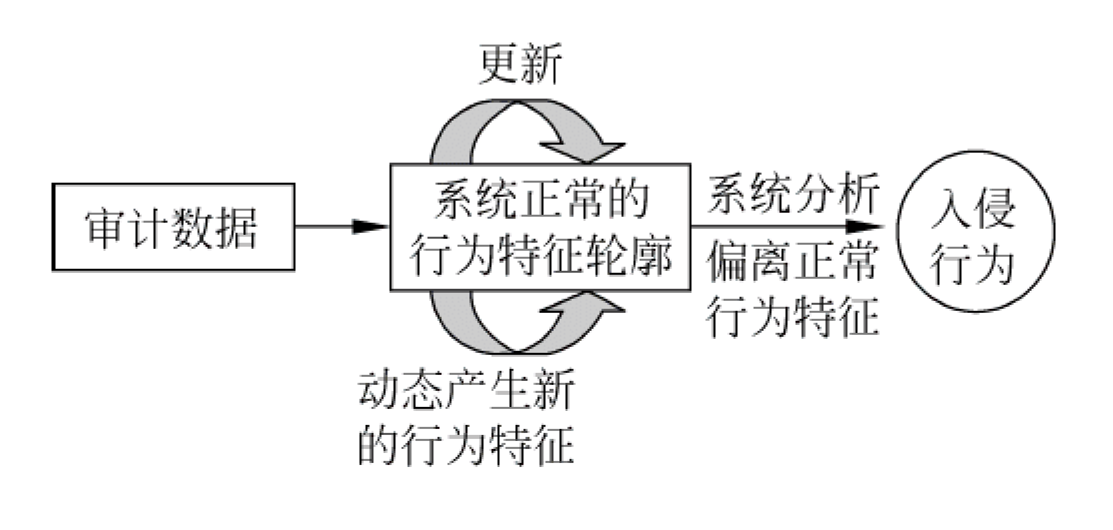


图 7.3 典型的异常检测系统

从异常检测的原理可以看出,该方法的技

术难点在于:“正常”行为特征轮廓的确定、特征量的选取、特征轮廓的更新。由于这几个因素的制约,异常检测的虚警率会很高,但对于未知的入侵行为的检测非常有效,同时它也是检测冒充合法用户的入侵行为的有效方法。此外,由于需要实时地建立和更新系统或用户的特征轮廓,因而所需的计算量很大,对系统的处理性能要求也很高。

2. 误用检测(misuse detection)

误用检测也被称为基于知识的检测。其基本前提是:假定所有可能的入侵行为都能被识别和表示。原理是:首先对已知的攻击方法进行攻击签名(攻击签名是指用一种特定的方式来表示已知的攻击模式)表示,然后根据已经定义好的攻击签名,通过判断这些攻击签名是否出现来判断入侵行为的发生与否。这种方法是通过直接判断攻击签名的出现与否来判断入侵行为的,从这一点来看,它是一种直接的方法。图 7.4 是典型的误用检测系统示意图。

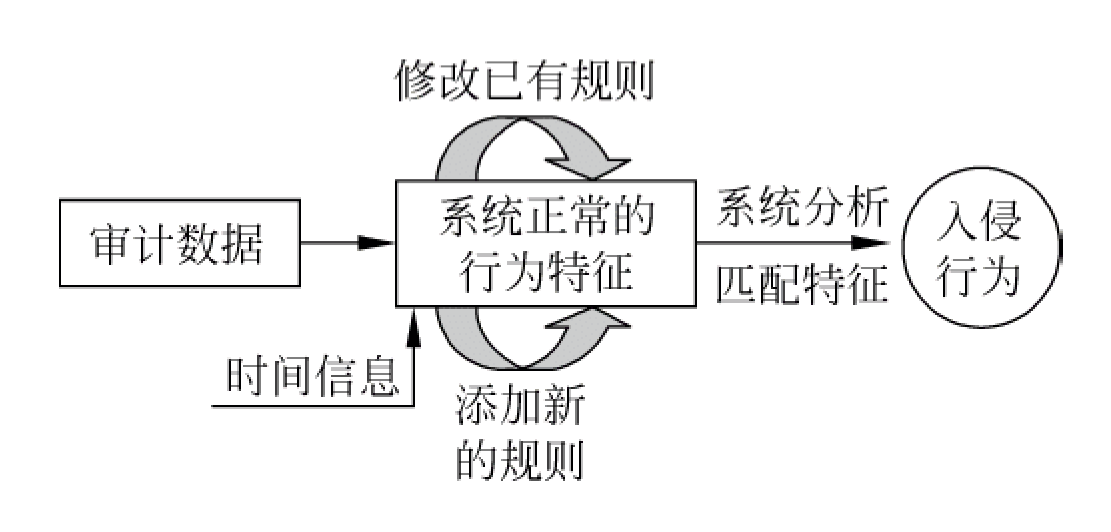


图 7.4　典型的误用检测系统

同样,误用检测也存在着影响检测性能的关键问题:攻击签名的正确表示。误用检测是根据攻击签名来判断入侵的,那么如何有效地根据对已知的攻击方法的了解,用特定的模式语言来表示这种攻击,即攻击签名的表示将是该方法的关键所在,尤其是攻击签名必须能够准确地表示入侵行为及其所有可能的变种,同时又不会把非入侵行为包含进来。

由于很大一部分的入侵行为利用的是系统的漏洞和应用程序的缺陷,因而通过分析攻击过程的特征、条件、排列以及事件间的关系,就可具体描述入侵行为的迹象。这些迹象不仅对分析已经发生的入侵行为有帮助,而且对即将发生的入侵行为也有预警作用,因为只要部分满足这些入侵迹象就意味着可能有入侵行为的发生。

误用检测是通过将收集到的信息与已知的攻击签名模式库进行比较,从而发现违背安全策略的行为。因此,它只需收集相关的数据,这样系统的负担就明显减少了。该方法类似于病毒检测系统,其检测的准确率和效率都比较高,而且这种技术比较成熟,国际上一些顶尖的入侵检测系统都采用的该方法,如 Cisco 的 NetRanger、IIS 的 Real Secure 以及 Axent 公司的 IntruderAlert 等。但是其检测的完备性则依赖于攻击签名知识库的不断更新和补充。另外,误用检测是通过匹配模式库来完成检测过程的,所以在计算处理上对系统的要求不是很高。

通常,这里所能检测到的入侵行为往往是利用操作系统的缺陷、应用软件的缺陷或网络协议实现上的缺陷等来实施的。误用检测通过检测那些与已知的入侵行为模式类似的行为或间接地违背系统安全策略的行为,来识别系统中的入侵活动。使用这种技术的入侵检测系统,可以避免系统以后再次遭受同样的入侵攻击行为,而且系统安全管理员能够很容易地知道系统遭受到了哪种攻击,并采取相应的行动。但是,知识库的维护需要对系统中的每一个缺陷都要进行详细的分析,这不仅是一个耗时的工作,而且关于攻击的知识依赖于操作系统、软件的版本、硬件平台以及系统中运行的应用程序等。

3. 采用两种技术混合的入侵检测

入侵检测的两种最常用技术在实现机理、处理机制上存在明显的不同,而且各自都有着

自身无法逾越的障碍，使得各自都有着某种不足。但是采用这两种技术混合的方案，将是一种理想的选择，这样可以做到优势互补。

7.4 入侵检测系统模型

比较有影响的入侵检测系统模型有：CIDF 模型、Denning 的通用入侵检测系统模型。其中，CIDF 模型是在对入侵检测系统进行规范化的进程中提出的，也是逐渐被入侵检测领域所采纳的模型；Denning 的通用入侵检测系统模型作为入侵检测发展历程中颇具影响力的实例，给入侵检测领域的研究带来了相当重要的启示。现在，很多的入侵检测系统研究原型都是基于这两个模型的，所以对其作一介绍。

7.4.1 入侵检测系统的 CIDF 模型

CIDF 模型是由 CIDF(Common Intrusion Detection Framework)工作组提出的。CIDF 工作组是由 Teresa Lunt 发起的，专门从事对入侵检测系统进行标准化的研究机构。它主要研究的是入侵检测系统的通用结构、入侵检测系统各组件间的通信接口问题、通用入侵描述语言以及不同入侵检测系统间通信问题等关于入侵检测的规范化问题。

CIDF 提出了一个入侵检测系统的通用模型(如图 7.5 所示)，它将入侵检测系统分为以下几个单元。

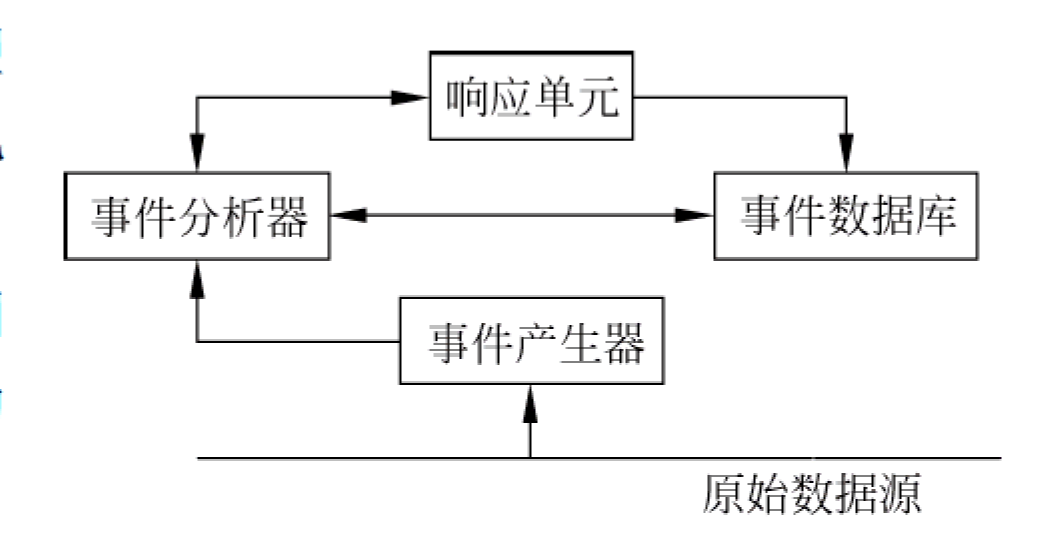


图 7.5 CIDF 模型

(1) 事件产生器(event generators)，即检测器，它从整个计算环境中获得事件，并向系统的其他部分提供此事件；

(2) 事件分析器(event analyzers)，分析得到的数据，并产生分析结果；

(3) 响应单元(response units)，对分析结果作出反应的功能单元，它可以作出切断连接、改变文件属性等反应，甚至发动对攻击者的反击，也可以只是简单的报警；

(4) 事件数据库(event databases)，存放各种中间和最终数据的地方的总称，它可以是复杂的数据库，也可以是简单的文本文件。各功能单元间的数据交换采用的是 CISL 语言。

CIDF 模型给出了入侵检测系统的一个基本框架。一般地，入侵检测系统由这些功能模块组成。在具体实现上，由于各种网络环境的差异以及安全需求的不同，因而在实际的结构上存在一定程度的差别。

7.4.2 Denning 的通用入侵检测系统模型

Dorothy E. Denning 于 1987 年提出了一个通用的入侵检测模型(如图 7.6 所示)。该模型由以下 6 个主要部分组成：主体、客体、审计记录、行为轮廓、异常记录及活动规则。

在该模型中，主体是指目标系统上活动的实体，通常指的是用户，也可能是代表用户行为的系统进程，或者是系统自身。主体的所有行为都是通过命令来实现的。客体是指系统资源，如文件、命令、设备等。它是主体行为的接受者。主体和客体没有明显的界限，往往在某一环境下的主体在另一环境下则会成为客体。

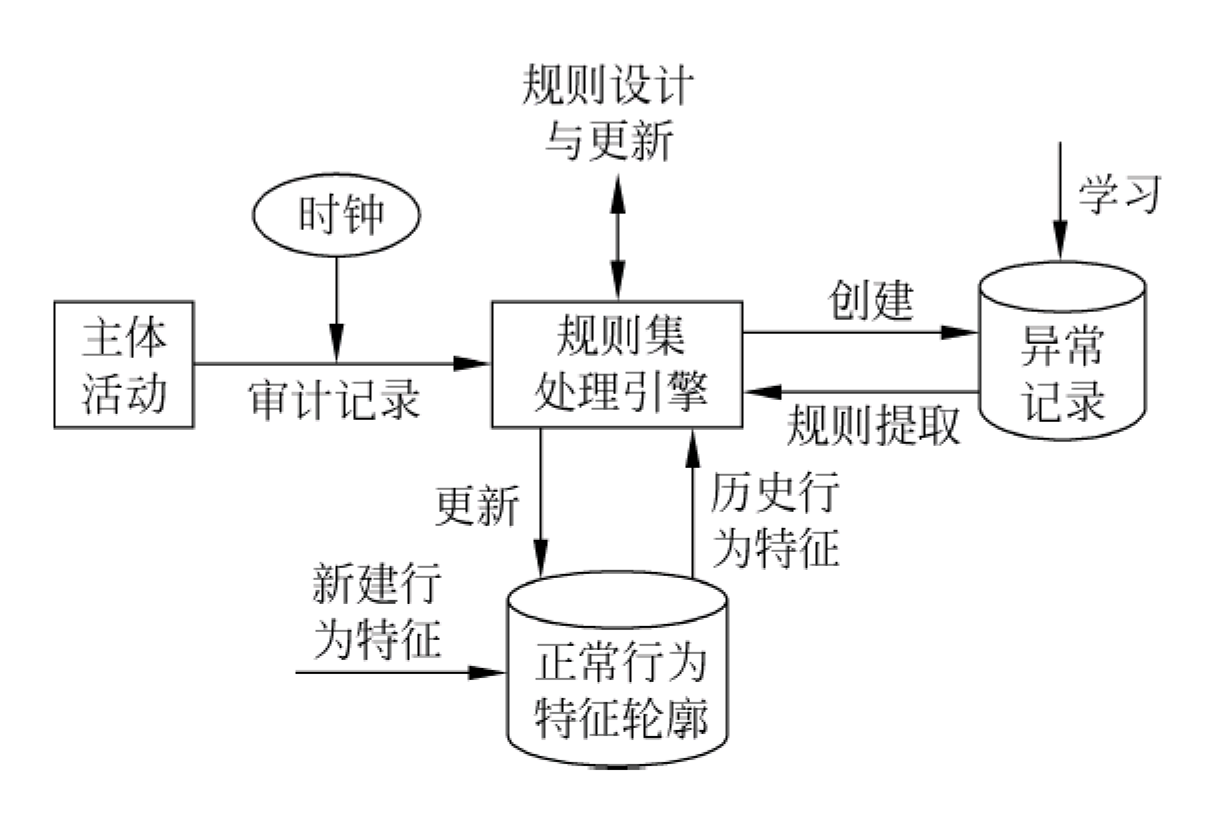


图 7.6　Denning 模型

审计记录是指主体对客体进行操作而在目标系统上产生的记录，如用户的登录、命令的执行、文件的访问等都会在系统中产生相应的记录。它是由“主体、活动、客体、异常条件、资源使用状况、时间戳”构成的六元组。其中，活动是指主体对客体的操作，如登录、退出、读、写等；异常条件是指主体活动出现异常情况时系统的状态；资源使用状况是指系统的资源消耗情况；时间戳是指活动发生的时间。

行为轮廓是描述主体对客体正常行为的模型，它包含有系统正常活动的各种相关信息。异常记录是指当系统检测到异常行为时产生的记录，由事件、时间戳、行为轮廓组成。活动规则是指系统判断是否是入侵的准则，以及当满足入侵条件时，系统所采取的相应的对策。

这个模型是个典型的异常检测的实现原型，对入侵检测的研究起着相当重要的推动作用。SRI 的 NIDES 的异常检测器就是基于该模型的。

7.5　分布式入侵检测系统

一方面，由于网络环境的分布性和开放性，使得我们要保护的目标主机和网络在数量和层次上将不再局限在很有限的范围内，而且不断发展的网络技术使得攻击手段也在不断推陈出新，这样，对入侵行为的检测将面临更大的挑战。另一方面，单一机制的入侵检测系统存在着自身难以克服的缺陷，无法满足日益苛刻的安全需求。这使得人们在深入研究的同时不得不另辟蹊径。分布式入侵检测系统就是这一时期的产物，它的出现为人们提供了新的安全解决方案。

分布式入侵检测系统是采用基于主机的和基于网络的入侵检测系统相结合的综合方案，这样既可以克服基于主机的入侵检测系统和基于网络的入侵检测系统的各自不足，又可以充分发挥它们各自的优势，从而实现对被保护目标的最佳防护。图 7.7 是分布式入侵检测系统的组成框图。

由图 7.7 可以看出，该系统的主要功能部件有网络引擎、主机代理、分析系统、管理控制系统、存储系统、响应系统等。网络引擎主要是从网络流量中获取原始数据包，并对其进行预处理，并将预处理后的数据发送给分析系统；主机代理则是从受保护的主机系统获取审计数据，并对其进行预处理，将处理过的数据送往分析系统；分析系统对预处理后的数据进行分析，根据不同的数据特点建立相应的检测模型，即采用不同的检测算法对数据进行分析

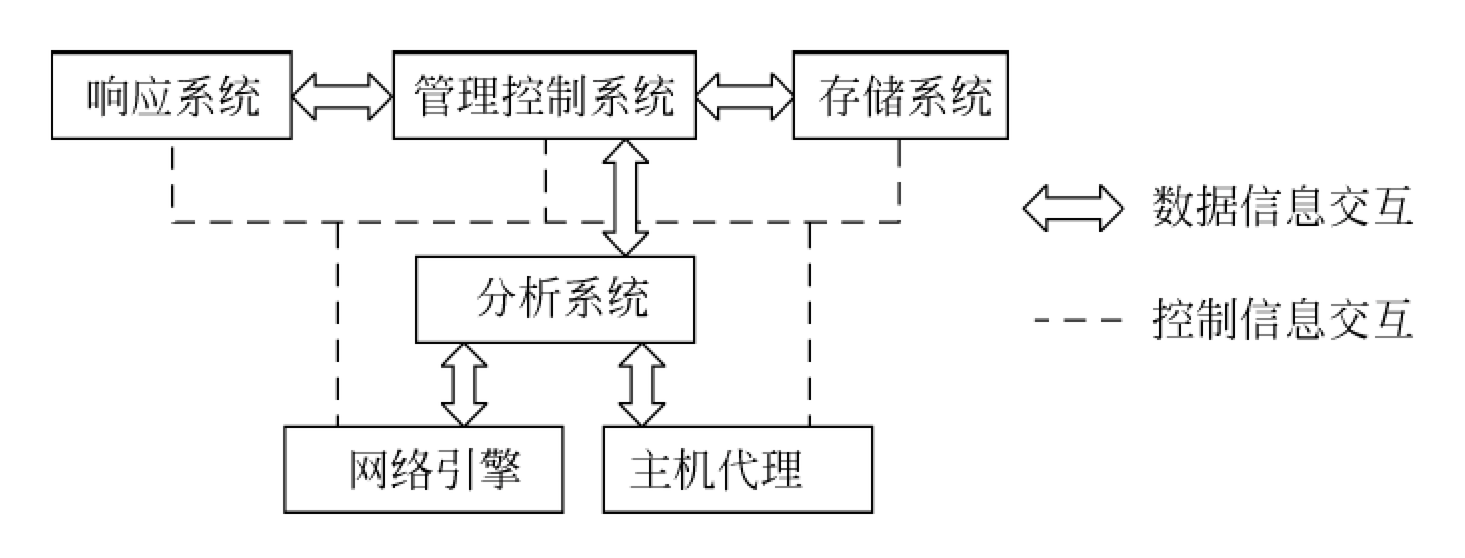


图 7.7　分布式入侵检测系统组成框图

处理，并将分析结果送到管理控制系统；管理控制系统是整个系统同用户交互的窗口，它提供各种管理控制信息，并协调其他部件的工作；存储系统是用来对各种结果进行存储的地方，并提供灵活的数据维护、处理和查询服务，同时也是一个安全的日志系统；响应系统则是对确认的入侵行为采取相应措施的子系统。从所采用的技术角度来看，分布式入侵检测系统的检测机制是误用检测和异常检测并举的方案。

一个典型的分布式入侵检测系统在实际网络环境下的部署如图 7.8 所示。在图 7.8 中，防火墙内外都设置了网络引擎，这样就可以充分利用基于网络的 IDS 的优点，实时地进行攻击企图的识别，并可将其阻断在防火墙之外。同时，还可监控透过防火墙的攻击行为，为及时地更新防火墙的配置提供依据。对于主机代理的设置则是要根据具体的安全防护策略来进行。这样，就可以最大限度地发挥不同类型的 IDS 的优势，实现对被保护网络的最大安全化。

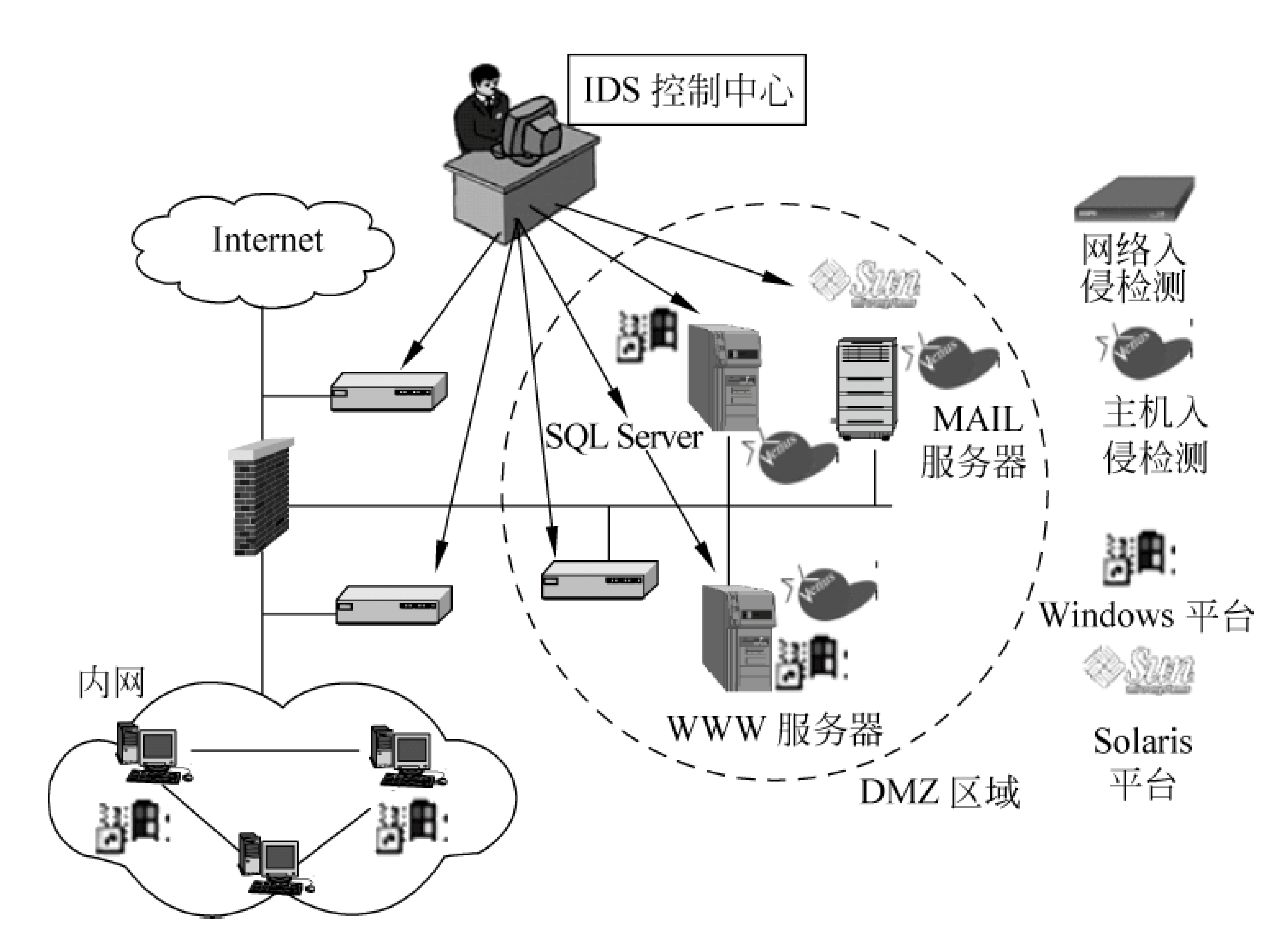


图 7.8　分布式入侵检测系统在实际网络环境下的部署

7.6　入侵检测技术的发展趋势

随着入侵检测技术的发展，成型的产品已陆续应用到实践中。人们在完善原有技术的基础上，又在研究新的检测方法，如数据融合技术、主动的自主代理方法、智能技术以及免疫

学原理的应用等。其主要的发展方向可概括为：

(1) 大规模分布式入侵检测。传统的入侵检测技术一般只局限于单一的主机或网络框架，显然不能适应大规模网络的监测，不同的入侵检测系统之间也不能协同工作。因此，必须发展大规模的分布式入侵检测技术。

(2) 宽带高速网络的实时入侵检测技术。大量高速网络的不断涌现，各种宽带接入手段层出不穷，如何实现高速网络下的实时入侵检测成为一个现实的问题。

(3) 入侵检测的数据融合技术。目前的IDS还存在着很多缺陷。首先，目前的技术还不能对付训练有素的黑客的复杂攻击。其次，系统的虚警率太高。最后，系统对大量的数据处理，非但无助于解决问题，还降低了处理能力。数据融合技术是解决这一系列问题的好方法。

(4) 与网络安全技术相结合，结合防火墙、病毒防护以及电子商务技术，提供完整的网络安全保障。

课后习题

填空题

1. (　　)是一种对网络传输进行即时监视，在发现可疑传输时发出警报或者采取主动反应措施的网络安全设备。
2. 按分析技术分类，入侵检测系统可分为(　　)和(　　)。
3. 按数据来源分类，入侵检测系统可分为(　　)和(　　)。
4. CIDF通用模型入侵检测系统分为几个单元：(　　)、(　　)、(　　)、事件数据库。
5. 入侵的定义是：企图破坏资源的完整性、(　　)、(　　)的任何行为，也指违背系统安全策略的任何事件。

简答题

1. 什么是入侵检测系统？
2. IDS的主要功能有哪些？
3. 基于网络的入侵检测系统有哪些优点？
4. IDS的分类有哪些？
5. 入侵检测系统常用的检测方法有哪些？
6. 今后的入侵检测技术大致有哪几个发展趋势？

第 8 章 VPN 技术

8.1 什么是虚拟专用网

随着企业网应用的不断扩大,企业网的范围也不断扩大,从本地到跨地区、跨城市,甚至是跨国家的网络。但采用传统的广域网建立企业专网,往往需要租用昂贵的跨地区数字专线。同时 Internet 已遍布各地,物理上各地的 Internet 都是连通的,但 Internet 是对社会开放的,如果企业的信息要通过公众信息网进行传输,在安全性上存在着很多问题。那么,该如何利用现有的公众信息网建立安全的企业专有网络呢?为了解决上述问题,人们提出了虚拟专用网(Virtual Private Network,VPN)的概念。

虚拟专用网(VPN)被定义为通过一个公用网络(通常是因特网)建立一个临时的、安全的连接,是一条穿过混乱的公用网络的安全、稳定的隧道。虚拟专用网是对企业内部网的扩展。虚拟专用网可以帮助远程用户、公司分支机构、商业伙伴及供应商同公司的内部网建立可信的安全连接,并保证数据的安全传输。虚拟专用网可用于不断增长的移动用户的全球因特网接入,以实现安全连接;可用于实现企业网站之间安全通信的虚拟专用线路,用于经济有效地连接到商业伙伴和用户的安全外联网虚拟专用网。

目前很多单位都面临着这样的挑战:分公司、经销商、合作伙伴、客户和外地出差人员要求随时经过公用网访问公司的资源,这些资源包括:公司的内部资料、办公 OA、ERP 系统、CRM 系统、项目管理系统等。现在很多公司通过使用 IPSec VPN 来保证公司总部和分支机构以及移动工作人员之间的安全连接。

8.2 VPN 的基本功能

虚拟专用网的重点在于建立安全的数据通道,构造这条安全通道的协议必须具备以下功能:

(1) 保证数据的真实性,通信主机必须是经过授权的,要有抵抗地址冒认(IPSpoofing)的能力。

(2) 保证数据的完整性,接收到的数据必须与发送时的一致,要有抵抗不法分子篡改数据的能力。

(3) 保证通道的机密性,提供强有力的加密手段,必须使偷听者不能破解拦截到的通道数据。

(4) 提供动态密钥交换功能,提供密钥中心管理服务器,必须具备防止数据重演的功能,保证通道不能被重演。

(5) 提供安全防护措施和访问控制，要有抵抗黑客通过 VPN 通道攻击企业网络的能力，并且可以对 VPN 通道进行访问控制。

8.3 VPN 所需的安全技术

VPN 主要采用四项技术来保证安全，这四项技术分别为：

(1) 隧道技术(tunneling)；

(2) 加解密技术(encryption & decryption)；

(3) 密钥管理技术(key management)；

(4) 认证技术(authentication)。

8.3.1 隧道技术

隧道技术是一种通过使用互联网络的基础设施在网络之间传递数据的方式。使用隧道传递的数据(或负载)可以是不同协议的数据帧或包。隧道协议将其他协议的数据帧或包重新封装然后通过隧道发送。新的帧头提供路由信息，以便通过互联网传递被封装的负载数据。

这里所说的隧道类似于点到点的连接。这种方式能够使来自许多信息源的网络业务在同一个基础设施中通过不同的隧道进行传输。隧道技术使用点对点通信协议代替了交换连接，通过路由网络来连接数据地址。隧道技术允许授权移动用户或已授权的用户在任何时间、任何地点访问企业网络。

通过隧道的建立，可实现：

(1) 将数据流强制送到特定的地址；

(2) 隐藏私有的网络地址；

(3) 在 IP 网上传递非 IP 数据包；

(4) 提供数据安全支持，

近来出现了一些新的隧道技术，并在不同的系统中得到运用和拓展。为创建隧道，隧道的客户机和服务器双方必须使用相同的隧道协议。隧道技术可分别以第 2 层或第 3 层隧道协议为基础。第 2 层隧道协议对应于 OSI 模型的数据链路层，使用帧作为数据交换单位。PPTP(点对点隧道协议)、L2TP(第二层隧道协议)和 L2F(第 2 层转发协议)都属于第 2 层隧道协议，是将用户数据封装在点对点协议(PPP)帧中通过互联网发送。第 3 层隧道协议对应于 OSI 模型的网络层，使用包作为数据交换单位。IPIP(IP over IP)以及 IPSec 隧道模式属于第 3 层隧道协议，是将 IP 包封装在附加的 IP 包头中，通过 IP 网络传送。无论哪种隧道协议都是由传输的载体、不同的封装格式以及用户数据包组成的。它们的本质区别在于，用户的数据包是被封装在哪种数据包中在隧道中传输。下面分别介绍这几种常用的隧道协议。

1. 点对点隧道协议(PPTP)

PPTP(Point to Point Tunneling Protocol)提供 PPTP 客户机和 PPTP 服务器之间的加密通信。PPTP 是 PPP 协议的一种扩展。它提供了一种在互联网上建立多协议的安全虚拟专用网(VPN)的通信方式。远端用户能够透过任何支持 PPTP 的 ISP 访问公司的专

用网。

通过 PPTP，客户可采用拨号方式接入公用 IP 网。拨号用户首先按常规方式拨到 ISP 的接入服务器(NAS)，建立 PPP 连接；在此基础上，用户进行二次拨号建立到 PPTP 服务器的连接，该连接称为 PPTP 隧道，实质上是基于 IP 协议的另一个 PPP 连接，其中的 IP 包可以封装多种协议数据，包括 TCP/IP、IPX 和 NetBEUI。PPTP 采用了基于 RSA 公司 RC4 的数据加密方法，保证了虚拟连接通道的安全。对于直接连到互联网的用户则不需要 PPP 的拨号连接，可以直接与 PPTP 服务器建立虚拟通道。PPTP 把建立隧道的主动权交给了用户，但用户需要在其 PC 上配置 PPTP，这样做既增加了用户的工作量，又会给网络带来隐患。另外，PPTP 只支持 IP 作为传输协议。

2. 第二层转发协议 L2F

L2F(Layer Two Forwarding protocol)是由 Cisco 公司提出的可以在多种介质，如 ATM、帧中继、IP 网上建立多协议的安全虚拟专用网的通信。远端用户能通过任何拨号方式接入公用 IP 网，首先按常规方式拨到 ISP 的接入服务器(NAS)，建立 PPP 连接；NAS 根据用户名等信息，建立直达 HGW 服务器的第二重连接。在这种情况下，隧道的配置和建立对用户是完全透明的。

3. 第二层隧道协议 L2TP

L2TP(Layer Two Tunneling Protocol)结合了 L2F 和 PPTP 的优点，允许用户从客户端或访问服务器端建立 VPN 连接。L2TP 是把链路层的 PPP 帧装入公用网络设施，如 IP、ATM、帧中继中进行隧道传输的封装协议。

Cisco、Ascend、Microsoft 和 RedBack 公司的专家们在修改了十几个版本后，终于在 1999 年 8 月公布了 L2TP 的标准 RFC2661。目前用户拨号访问 Internet 时，必须使用 IP 协议，并且其动态得到的 IP 地址也是合法的。L2TP 的好处在于支持多种协议，用户可以保留原有的 IPX、Appletalk 等协议或公司原有的 IP 地址。L2TP 还解决了多个 PPP 链路的捆绑问题，PPP 链路捆绑要求其成员均指向同一个 NAS，L2TP 则允许在物理上连接到不同 NAS 的 PPP 链路，在逻辑上的终点为同一个物理设备。L2TP 扩展了 PPP 连接，在传统的方式中用户通过模拟电话线或 ISDN/ADSL 与网络访问服务器建立一个第 2 层的连接，并在其上运行 PPP，第 2 层连接的终点和 PPP 会话的终点均设在同一个设备上(如 NAS)。L2TP 作为 PPP 的扩充提供了更强大的功能，包括允许第 2 层连接的终点和 PPP 会话的终点分别设在不同的设备上。

L2TP 主要由 LAC(L2TP Access Concentrator)和 LNS(L2TP Network Server)构成。LAC 支持客户端的 L2TP，发起呼叫，接收呼叫和建立隧道；LNS 是所有隧道的终点。在传统的 PPP 连接中，用户拨号连接的终点是 LAC，而 L2TP 能把 PPP 协议的终点延伸到 LNS。

用户通过公用电话网或 ISDN 拨号呼叫本地接入服务器 LAC。LAC 接受呼叫并进行基本的识别过程，这一过程可以采用几种标准，如域名、呼叫线路识别(CLID)或拨号 ID 业务(DNIS)等。

L2TP 方式给服务提供商和用户带来了许多方便。用户不需要在 PC 上安装专门的客户端软件，企业网可以使用未注册的 IP 地址，并在本地管理认证数据库，从而降低了应用成本和培训维护费用。

与 PPTP 和 L2F 相比，L2TP 的优点在于提供了差错和流量控制；L2TP 使用 UDP 封装和传送 PPP 帧。面向无连接的 UDP 无法保证网络数据的可靠传输，L2TP 使用 Nr(下一个希望接受的信息序列号)和 Ns(当前发送的数据包序列号)字段进行流量和差错控制。双方通过序列号来确定数据包的顺序和缓冲区，一旦丢失数据，根据序列号可以进行重发。

作为 PPP 的扩展协议，L2TP 支持标准的安全特性 CHAP 和 PAP，可以进行用户身份认证。L2TP 定义了控制包的加密传输，每个被建立的隧道分别生成一个独一无二的随机钥匙，以便对付欺骗性的攻击，但是它对传输中的数据并不加密。

4. 通用路由封装

通用路由封装(Generic Routing Encapsulation，GRE)在 RFC1701/RFC1702 中定义，它规定了怎样用一种网络层协议去封装另一种网络层协议的方法。GRE 的隧道由两端的源 IP 地址和目的 IP 地址来定义，它允许用户使用 IP 封装 IP、IPX、AppleTalk，并支持全部的路由协议，如 RIP、OSPF、IGRP、EIGRP。通过 GRE，用户可以利用公用 IP 网络连接 IPX 网络和 AppleTalk 网络，还可以使用保留地址进行网络互联，或对公网隐藏企业网的 IP 地址。

GRE 的包头包含了协议类型(用于标明乘客协议的类型)，其校验和包括了 GRE 的包头和完整的乘客协议与数据，其密钥用于接收端验证接收的数据，其序列号用于接收端数据包的排序和差错控制，路由信息(用于本数据包的路由)。

GRE 只提供了数据包的封装，它没有防止网络侦听和攻击的加密功能。所以在实际环境中它常和 IPSec 一起使用，由 IPSec 为用户数据的加密，给用户提供更好的安全服务。

8.3.2 加密技术

IPSec 通过 ISAKMP/IKE/Oakley 协商确定几种可选的数据加密算法，如 DES 、3DES 等。DES 密钥长度为 56 位，容易被破译，3DES 使用三重加密增加了安全性。当然国外还有更好的加密算法，但国外禁止出口高位加密算法。基于同样理由，国内也禁止重要部门使用国外算法。国内算法不对外公开，被破解的可能性极小。图 8.1 展示了隧道和加密技术在 VPN 中是如何应用的。

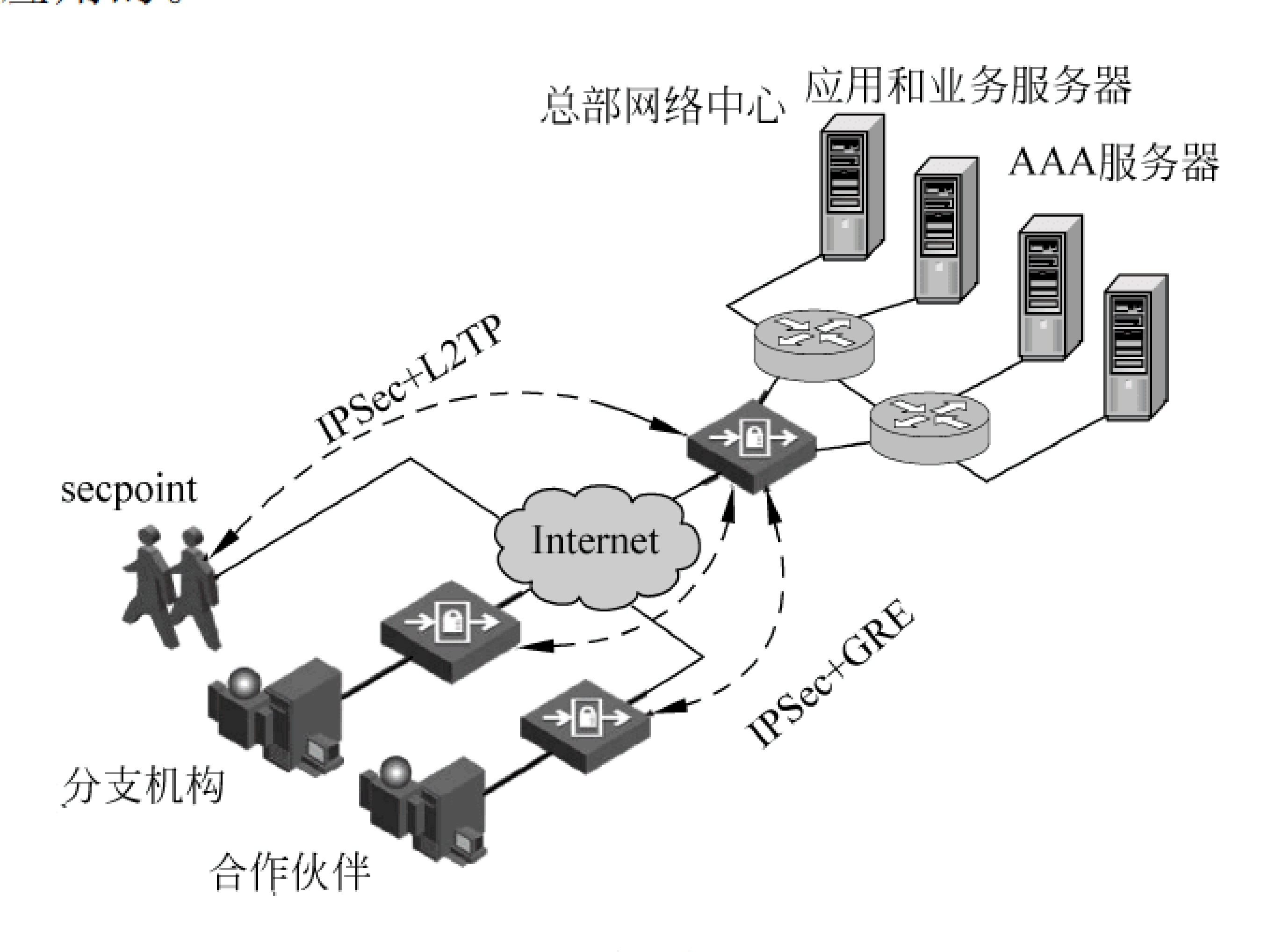


图 8.1 隧道与加密的应用

8.3.3 密钥分发和管理

VPN 中密钥的分发与管理非常重要。密钥的分发有两种方法：一种是通过手工配置的方式，另一种是采用密钥交换协议动态分发。手工配置的方法由于密钥更新困难，只适合于简单网络的情况。密钥交换协议采用软件方式动态生成密钥，适合于复杂网络的情况且密钥可快速更新，可以显著提高 VPN 的安全性。目前主要的密钥交换与管理标准有 IKE（互联网密钥交换）、SKIP（互联网简单密钥管理）和 Oakley。

8.3.4 身份认证技术

认证技术防止数据的伪造和被篡改，它采用一种称为“摘要”的技术。“摘要”技术主要采用 hash 函数将一段长的报文通过函数变换映射为一段短的报文即摘要。由于 hash 函数的特性，两个不同的报文具有相同的摘要几乎不可能。该特性使得摘要技术在 VPN 中有两个用途：验证数据的完整性、用户认证。

8.4 VPN 的分类

根据不同的需要，可以构造不同类型的 VPN。不同商业环境对 VPN 的要求和 VPN 所起的作用不同。这里分三种情况说明 VPN 的用途。

（1）内部 VPN：指在公司总部和其分支机构之间建立的 VPN。

内部网是通过公共网络将某一个组织的各个分支机构的 LAN 连接而成的网络。这种类型的 LAN 到 LAN 的连接所带来的风险最小，因为公司通常认为他们的分支机构是可信的，这种方式连接而成的网络被称为 Intranet，可看作是公司网络的扩展，其拓扑如图 8.2 所示。

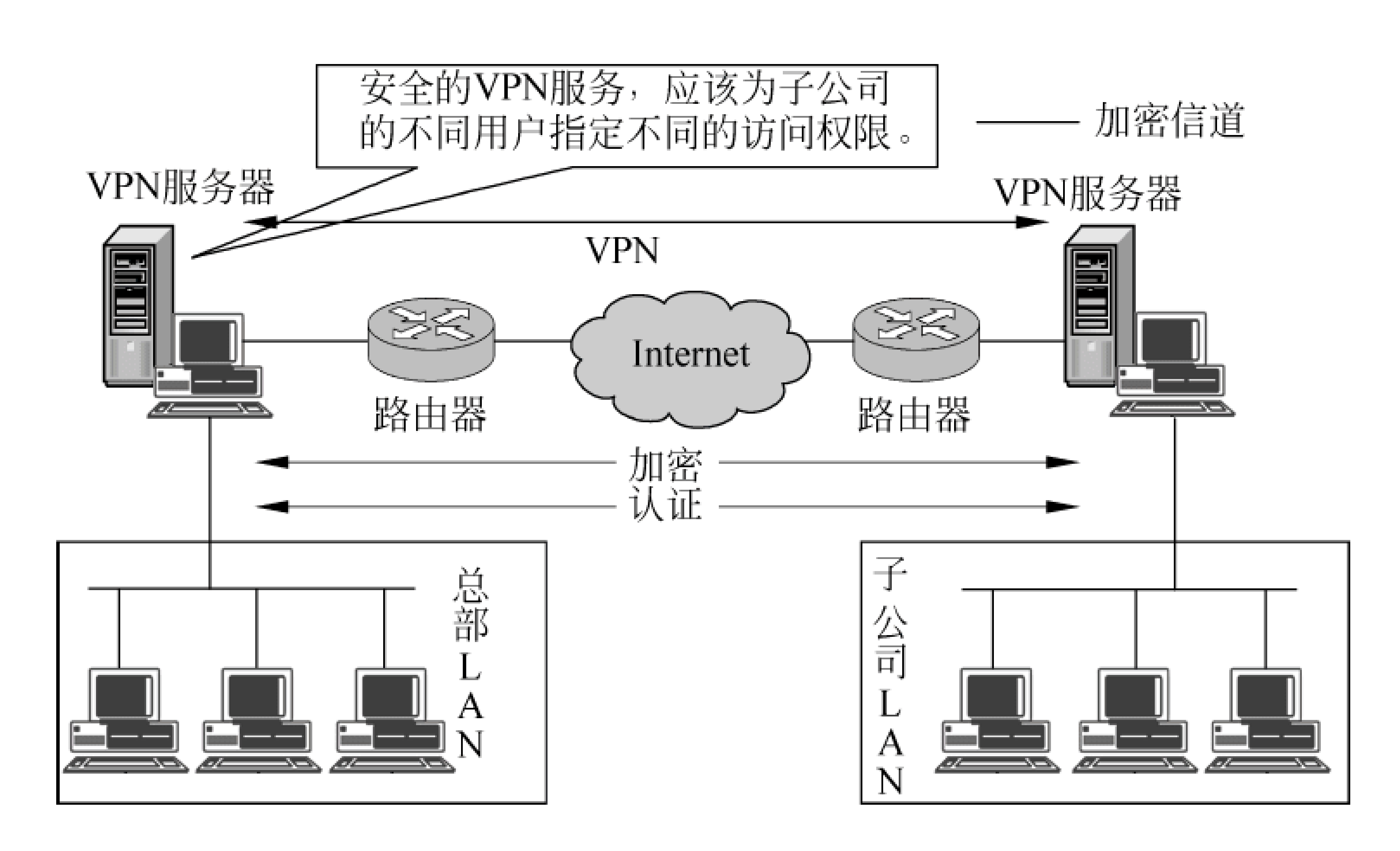


图 8.2 内部网 VPN 拓扑图

当一个数据传输通道的两个端点被认为是可信的时候，可以选择内部网 VPN 解决方案。安全性主要在于加强两个 VPN 服务器之间加密和认证的手段。

（2）远程访问 VPN：指在公司总部和远地雇员之间建立的 VPN。

典型的远程访问 VPN 是用户通过本地的信息提供商(ISP)登录到 Internet 上，并在现在的办公室和公司内部网之间建立一条加密通道。有较高安全度的远程访问 VPN 应能截获特定主机的信息流，有加密、身份认证和过滤等功能，如图 8.3 所示。

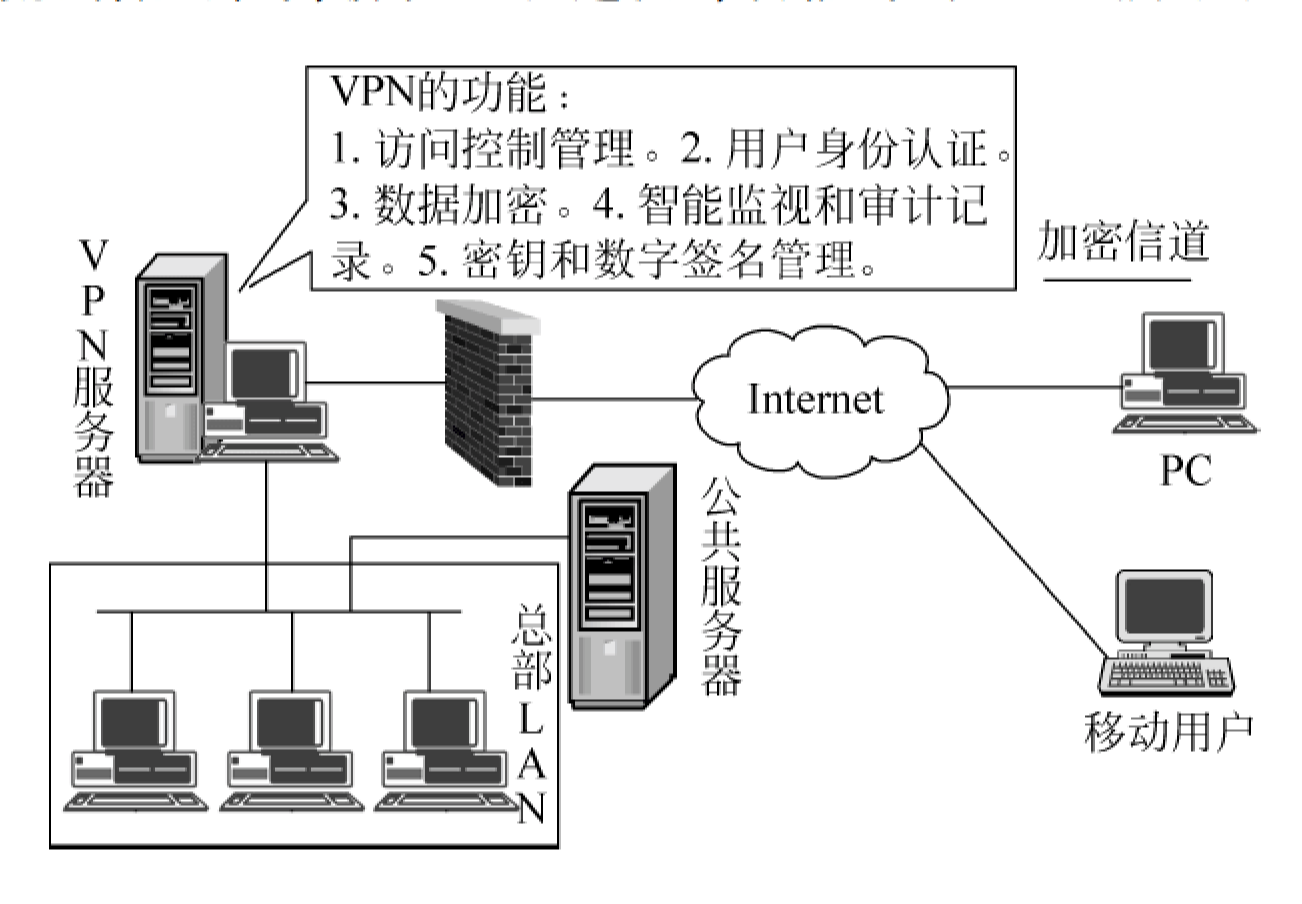


图 8.3　远程访问 VPN

(3) 外联网 VPN：指公司与商业伙伴、客户之间建立的 VPN。

外联网 VPN 为公司商业伙伴、客户和在远地的雇员提供安全性。外联网 VPN 的主要目标是保证数据在传输过程中不被修改，保护网络资源不受外部威胁。外联网 VPN 应是一个由加密、认证和访问控制功能组成的集成系统。通常将公司的 VPN 代理服务器放在一个不能穿透的防火墙之后，防火墙阻止来历不明的信息传输。所有经过过滤后的数据通过一个唯一的入口传到 VPN 服务器，VPN 再根据安全策略进一步过滤，其拓扑如图 8.4 所示。

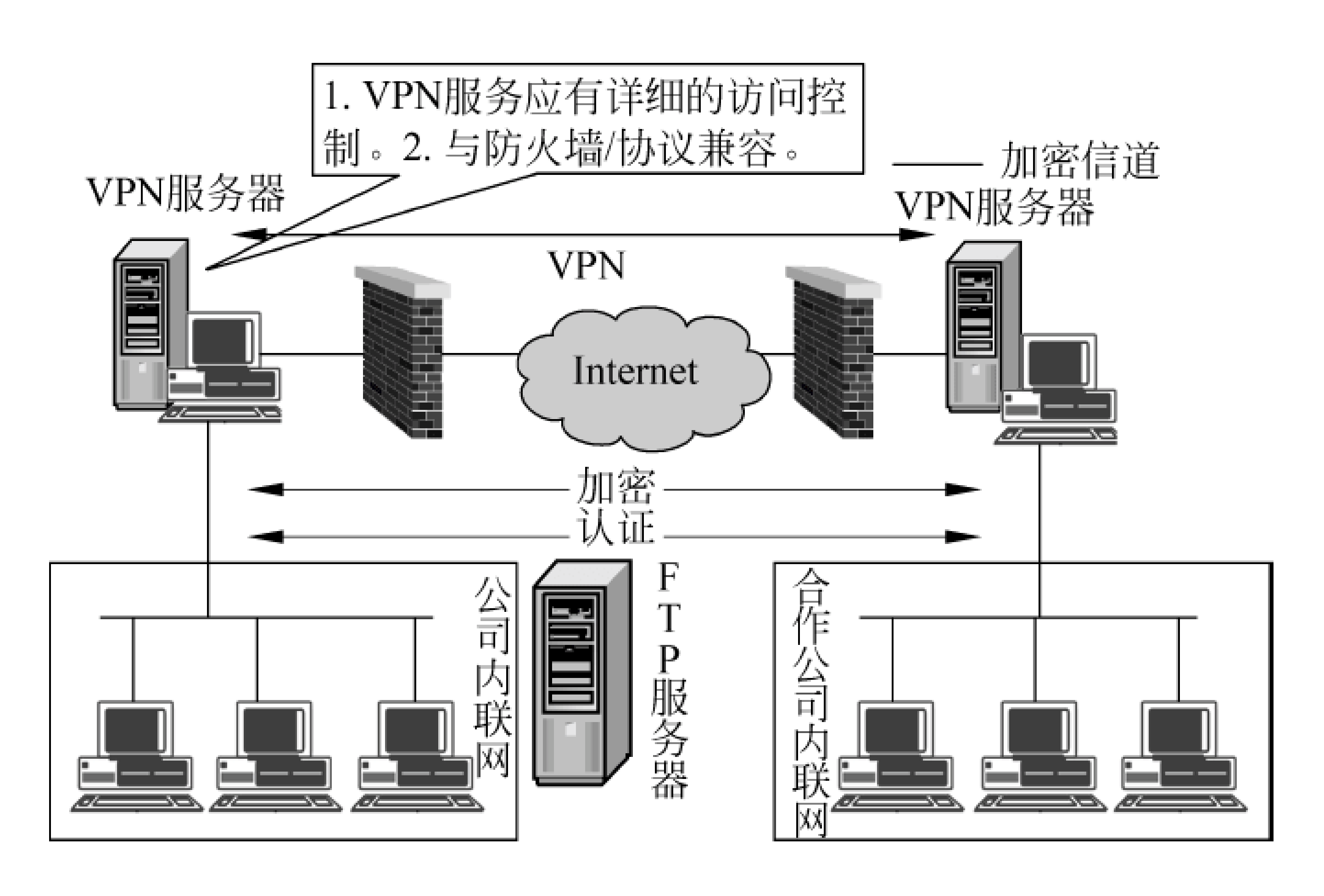


图 8.4　外联网 VPN 拓扑图

8.5　IP 安全协议

IP 安全协议(IP Security，IPSec)实际上是一套协议包而不是一个独立的协议，这一点对于认识 IPSec 是很重要的。从 1995 年开始 IPSec 的研究以来，IETF IPSec 工作组在它的

主页上发布了几十个 Internet 草案文献和 12 个 RFC 文件。其中,比较重要的有 RFC2409 IKE(互联网密钥交换)、RFC2401 IPSec 协议、RFC2402 AH 验证包头、RFC2406 ESP 加密数据等文件。

IPSec 安全体系包括 3 个基本协议:AH 协议为 IP 包提供信息源验证和完整性保证;ESP 协议提供加密机制;密钥管理协议(ISAKMP)提供双方交流时的共享安全信息。ESP 和 AH 协议都有相关的一系列支持文件,规定了加密和认证的算法。最后,解释域(DOI)通过一系列命令、算法、属性和参数连接所有的 IPSec 组文件。

8.5.1 IPSec 的安全特性

(1) 不可否认性,可以证实消息发送方是唯一可能的发送者,发送者不能否认发送过消息。“不可否认性”是采用公钥技术的一个特征,当使用公钥技术时,发送方用私钥产生一个数字签名随消息一起发送,接收方用发送者的公钥来验证数字签名。由于在理论上只有发送者才唯一拥有私钥,也只有发送者才可能产生该数字签名,所以只要数字签名通过验证,发送者就不能否认曾发送过该消息。但“不可否认性”不是基于认证的共享密钥技术的特征,因为在基于认证的共享密钥技术中,发送方和接收方掌握相同的密钥。

(2) 反重播性,确保每个 IP 包的唯一性,保证信息万一被截取复制后,不能再被重新利用、重新传输回目的地址。该特性可以防止攻击者截取破译信息后,再用相同的信息包冒取非法访问权(即使这种冒取行为发生在数月之后)。

(3) 数据完整性,防止传输过程中数据被篡改,确保发出数据和接收数据的一致性。IPSec 利用 hash 函数为每个数据包产生一个加密检查和,接收方在打开包前先计算检查和,若包遭篡改导致检查和不相符,数据包即被丢弃。

(4) 数据可靠性(加密),在传输前,对数据进行加密,可以保证在传输过程中,即使数据包遭截取,信息也无法被读。该特性在 IPSec 中为可选项,与 IPSec 策略的具体设置相关。认证数据源发送信任状态,由接收方验证信任状态的合法性,只有通过认证的系统才可以建立通信连接。

8.5.2 基于电子证书的公钥认证

一个架构良好的公钥体系,在信任状态的传递中不造成任何信息外泄,能解决很多安全问题。IPSec 与特定的公钥体系相结合,可以提供基于电子证书的认证。公钥证书认证在 Windows 2003 中,适用于对非 Windows 2003 主机、独立主机,非信任域成员的客户机,或者不运行 Kerberos v5 认证协议的主机进行身份认证。

8.5.3 预置共享密钥认证

IPSec 也可以使用预置共享密钥进行认证。预共享意味着通信双方必须在 IPSec 策略设置中就共享的密钥达成一致。之后在安全协商过程中,信息在传输前使用共享密钥加密,接收端使用同样的密钥解密,如果接收方能够解密,即被认为可以通过认证。但在 Windows 2003 IPSec 策略中,这种认证方式被认为不够安全而一般不推荐使用。

8.5.4 公钥加密

IPSec 的公钥加密用于身份认证和密钥交换，每个用户拥有一个密钥对，其中私钥仅为其个人所知，公钥则可分发给任意需要与之进行加密通信的人。例如，A 想要发送加密信息给 B，则 A 需要用 B 的公钥加密信息，之后只有 B 才能用他的私钥对该加密信息进行解密。虽然密钥对中两把钥匙彼此相关，但要想从其中一把推导出另一把，以目前计算机的运算能力来看，这种做法几乎完全不现实。因此，在这种加密法中，公钥可以广为分发，而私钥则需要仔细地妥善保管。

8.5.5 hash 函数和数据完整性

hash 信息验证码（Hash Message Authentication Codes，HMAC）验证接收消息和发送消息的完全一致性（完整性）。这在数据交换中非常关键，尤其当传输媒介如公共网络中不提供安全保证时更显其重要性。

HMAC 结合 hash 算法和共享密钥提供完整性。hash（散列）通常也被当成是数字签名，但这种说法不够准确，两者的区别在于：散列使用共享密钥，而数字签名基于公钥技术。hash 算法也称为消息摘要或单向转换。称它为单向转换是因为：

（1）双方必须在通信的两个端头处各自执行 hash 函数计算。

（2）使用 hash 函数很容易从消息计算出消息摘要，但其逆向反演过程以目前计算机的运算能力几乎不可实现。

散列本身就是所谓加密检查和/或消息完整性编码（Message Integrity Code，MIC），通信双方必须各自执行函数计算来验证消息。举例来说，发送方首先使用 HMAC 算法和共享密钥计算消息检查和，然后将计算结果 A 封装进数据包中一起发送；接收方再对所接收的消息执行 HMAC 计算得出结果 B，并将 B 与 A 进行比较。如果消息在传输中遭篡改致使 B 与 A 不一致，接收方丢弃该数据包。

有两种最常用的 hash 函数：

（1）HMAC-MD5。MD5（消息摘要 5）基于 RFC1321。MD5 对 MD4 做了改进，计算速度比 MD4 稍慢，但安全性能得到了进一步改善。MD5 在计算中使用了 64 个 32 位常数，最终生成一个 128 位的完整性检查和。

（2）HMAC-SHA。安全 hash 算法定义在 NIST FIPS 180-1，其算法以 MD5 为原型。SHA 在计算中使用了 79 个 32 位常数，最终产生一个 160 位完整性检查和。SHA 检查和长度比 MD5 更长，因此安全性也更高。

8.5.6 加密和数据可靠性

IPSec 使用的数据加密算法是 DES（数据加密标准）。DES 密钥长度为 56 位，在形式上是一个 64 位数。DES 以 64 位（8 字节）为分组对数据加密，每 64 位明文，经过 16 轮置换生成 64 位密文，其中每字节有 1 位用于奇偶校验，所以实际有效密钥长度是 56 位。IPSec 还支持 3DES 算法，3DES 可提供更高的安全性，但相应地，计算速度更慢。

8.5.7 密钥管理

1. 动态密钥更新

IPSec 策略使用“动态密钥更新”法来决定在一次通信中，新密钥产生的频率。动态密钥指在通信过程中，数据流被划分成一个个“数据块”，每一个“数据块”都使用不同的密钥加密，这可以保证万一攻击者中途截取了部分通信数据流和相应的密钥后，也不会危及所有其余的通信信息的安全。动态密钥更新服务由 Internet 密钥交换（Internet Key Exchange，IKE）提供。

IPSec 策略允许专家级用户自定义密钥生命周期。如果该值没有设置，则按默认时间间隔自动生成新密钥。

2. 密钥长度

密钥长度每增加一位，可能的密钥数就会增加一倍，相应地，破解密钥的难度也会随之呈指数级加大。IPSec 策略提供多种加密算法，可生成多种长度不等的密钥，用户可根据不同的安全需求加以选择。

3. Diffie-Hellman 算法

要启动安全通信，通信两端必须首先得到相同的共享密钥（主密钥），但共享密钥不能通过网络相互发送，因为这种做法极易泄密。

Diffie-Hellman 算法是用于密钥交换的最早最安全的算法之一。DH 算法的基本工作原理是：通信双方公开或半公开交换一些准备用来生成密钥的“材料数据”，在彼此交换过密钥生成“材料”后，两端可以各自生成出完全一样的共享密钥。在任何时候，双方都绝不交换真正的密钥。

通信双方交换的密钥生成“材料”，长度不等，“材料”长度越长，所生成的密钥强度也就越高，密钥破译就越困难。除进行密钥交换外，IPSec 还使用 DH 算法生成所有其他加密密钥。

8.5.8 IPSec 的好处

在防火墙或路由器中实现时，可以对所有跨越周界的流量实施强安全性。而公司内部或工作组不必招致与安全相关处理的负担，同时可以防止 IP 旁路。

IPSec 是在传输层之下，因此对应用透明，不必改变用户或服务器系统上的软件。对最终用户也是透明，无须训练用户，同时可以提供个人安全性。这对非现场工作人员以及在一个组织内为一个敏感应用建立一个安全的虚拟子网是有用的。

8.6 安全套接层

安全套接层（Secure Socket Layer，SSL）为 Netscape 所研发，用以保障在 Internet 上数据传输之安全，利用数据加密技术，可确保数据在网络传输过程中不会被截取及窃听。目前一般通用的规格为 40 位安全标准，美国则已推出 128 位更高安全标准，但限制出境。只要 3.0 版本以上的 IE 或 Netscape 浏览器即可支持 SSL。它已被广泛地用于 Web 浏览器与服务器之间的身份认证和加密数据传输。

SSL协议位于TCP/IP协议与各种应用层协议之间，为数据通信提供安全支持。SSL协议可分为两层：SSL记录协议，建立在可靠的传输协议(如TCP)之上，为高层协议提供数据封装、压缩、加密等基本功能的支持。SSL握手协议，建立在SSL记录协议之上，用于在实际的数据传输开始前，通信双方进行身份认证、协商加密算法、交换加密密钥等。

1. SSL协议提供的主要服务

(1) 认证用户和服务器，确保数据发送到正确的客户机和服务器；

(2) 加密数据以防止数据中途被窃取；

(3) 维护数据的完整性，确保数据在传输过程中不被改变。

2. SSL协议的工作流程

(1) 客户端向服务器发送一个开始信息"Hello"以便开始一个新的会话连接。

(2) 服务器根据客户的信息确定是否需要生成新的主密钥，如需要则服务器在响应客户的Hello信息时将包含生成主密钥所需的信息。

(3) 客户根据收到的服务器响应信息，产生一个主密钥，并用服务器的公开密钥加密后传给服务器。

(4) 服务器恢复该主密钥，并返回给客户一个用主密钥认证的信息，以此让客户认证服务器。

(5) 经认证的服务器发送一个提问给客户，客户则返回(数字)签名后的提问和其公开密钥，从而向服务器提供认证。

从SSL协议所提供的服务及其工作流程可以看出，SSL协议运行的基础是商家对消费者信息保密的承诺，这就有利于商家而不利于消费者。在电子商务初级阶段，由于运作电子商务的企业大多是信誉较高的大公司，因此这问题还没有充分暴露出来。但随着电子商务的发展，各中小型公司也参与进来，这样在电子支付过程中的单一认证问题就越来越突出。虽然在SSL3.0中通过数字签名和数字证书可实现浏览器和Web服务器双方的身份验证，但是SSL协议仍存在一些问题，比如，只能提供交易中客户与服务器间的双方认证，在涉及多方的电子交易中，SSL协议并不能协调各方的安全传输和信任关系。在这种情况下，Visa和MasterCard两大信用卡公组织制定了SET协议，为网上信用卡支付提供了全球性的标准。

3. HTTPS(Secure Hypertext Transfer Protocol)安全超文本传输协议

它是由Netscape开发并内置于其浏览器中，用于对数据进行压缩和解压操作，并返回网络上传送回的结果。HTTPS实际上应用了Netscape的完全套接字层(SSL)作为HTTP应用层的子层(HTTPS默认使用端口443)。SSL使用40位关键字作为RC4流加密算法，这对于商业信息的加密是合适的。HTTPS和SSL支持使用X.509数字认证，如果需要的话用户可以确认发送者是谁。

HTTPS是以安全为目标的HTTP通道，简单讲是HTTP的安全版。即HTTP下加入SSL层，HTTPS的安全基础是SSL。也就是说它的主要作用可以分为两种：一种是建立一个信息安全通道来保证数据传输的安全；另一种就是确认网站的真实性。

8.7 SSL VPN 与 IPSec VPN 安全比较

随着 SSL VPN 应用的逐渐加温，越来越多的企业开始采纳 SSL VPN 的网络架构，来解决企业的远程访问需求。但是自然有许多的观望者质疑 SSL VPN 的安全性和网络的兼容性。对于网络的兼容性，由于 IPSec 和 SSL 采取 Internet 网络中的不同网络层来进行安全加密处理，以建立网络安全通道，因此在网络的安全管理等级上，各有所长。以下分别从不同的角度来探讨这两种 VPN 应用的安全区别。

(1) 安全通道方面。IPSec 和 SSL 这两种安全协议，都有采用对称式和非对称式的加密算法来执行加密作业。在安全的通道比较上，并没有谁好谁坏之差，仅在于应用上的不同。例如美国的一家系统公司提供了四所医院及其相关医疗单位的网络系统和技术服务，采用了 SSL VPN 系统给 500 位医生和诊所，可以从远程来执行医疗操作系统，查询和更新病人的所有数据，但是他们仍然采用 IPSec VPN 来连接医院之间点对点的网络。

(2) 认证和权限控制管理方面。IPSec 使用数字凭证或是一组密钥来做认证，而 SSL 仅能使用数字凭证，如果都是采取数字凭证来认证，两者在认证的安全等级上就没有太大的差别。SSL 的认证，大多数的厂商都会建置硬件的标志，来提升认证的安全性。对于使用权限的控管，IPSec 可以支持选择，让网络封包过滤以阻隔某些特定的主机或应用系统。SSL 可以设定不同的使用者，执行不同的应用系统，它在管理和设定上比 IPSec 简单方便许多。

(3) 安全测试方面。IPSec VPN 已经有多年的发展，有许多的学术和非营利实验室，提供各种测试准则和服务，大多数的防火墙、VPN 厂商，都会以通过它的测试及认证为重要的基准。但 SSL VPN 在这方面，尚未有一个公正的测试准则。

(4) 应用系统的攻击方面。远程用户以 IPSec VPN 的方式与公司内部网络建立联机之后，内部网络所连接的应用系统，都是可以侦测得到的，这就提供了黑客攻击的机会。若是采取 SSL VPN 来联机，因为是直接开启应用系统，并没在网络层上连接，黑客不易侦测出应用系统内部网络，所受到的威胁也仅是所联机的这个应用系统，攻击机会相对就减少。

(5) 病毒入侵方面。一般企业在 Internet 入口处都会采取适当的防毒侦测措施。不论是 IPSec VPN 或 SSL VPN 联网，对于入口的病毒侦测效果是相同的，但是比较从远程客户端入侵的可能性，就会有所差别。采用 IPSec 联网，若是客户端计算机遭到病毒感染，这个病毒就有机会感染到内部网络所连接的每台计算机。相对于 SSL VPN 的联网，所感染的可能性会局限于这台主机，而且这个病毒必须是针对应用系统的类型，不同类型的病毒是不会感染到这台主机的。

(6) 防火墙上的通信端口方面，在 TCP/IP 的网络架构上，各式各样的应用系统会采取不同的通信协议，并且通过不同的协议来作为服务器和客户端之间的数据传输通道。以 E-mail 系统来说，发信和收信一般都是采取 SMTP 和 POP3 协议，而且两种协议都采用 port 25，若是从远程计算机来连接 E-mail 服务器，就必须在防火墙上开放 port 25，否则远程计算机是无法与 SMTP 和 POP3 主机沟通的。IPSec VPN 联机就会有这个困扰和安全顾虑。在防火墙上，每开启一个端口，就多一个黑客攻击机会。反观之，SSL VPN 就没有这方面的困扰。因为在远程主机与 SSL VPN 网关之间，采用 SSL 通信端口(port 443)来作为传输通

道，这个通信端口一般是作为 Web Server 对外的数据传输通道，因此，不需在防火墙上做任何修改，也不会因为不同应用系统的需求，而来修改防火墙上的设定，减少 IT 管理者的困扰。

IPSec VPN 和 SSL VPN 这两种 VPN 架构，从整体的安全等级来看，都能够提供安全的远程登录服务。但综上所述，SSL VPN 的易于使用性及安全层级都比 IPSec VPN 高。我们都知道，由于 Internet 的迅速扩展，针对远程安全登录的需求也日益提升。对于使用者而言，方便安全的解决方案才能真正符合需求。

8.8 VPN 技术应用案例

8.8.1 大学校园网 VPN 技术要求

(1) 身份验证。由于已经有了自己的统一身份认证系统，故在 VPN 方案中，对用户的身份认证必须使用已经存在的用户信息数据，或是直接与该校统一身份认证系统对接进行认证。

(2) 加密保护。要求对 VPN 隧道建立和用户通信都能进行加密，支持预共享密钥、数字证书的身份认证，提供动态密钥交换功能，支持 IPSec 隧道模式封装和传输模式封装，支持多种加密认证算法。加密速度快，能达到千兆通信，VPN 转发能达到 200Mb/s 以上。

(3) 方便安全的管理。要求在管理上能有多种方式。提供本地网络管理、telnet 管理、远程管理等多种管理方式，在以上方式中能对 VPN 安全策略、访问控制策略等进行调整。

(4) DHCP 支持。要求能给每一个接入 VPN 的用户动态分配一个校内 IP 地址，地址池能在 2000 个 IP 以上。并且得到的该地址可以与校内资源进行通信。

(5) 多种用户环境支持。支持专线宽带接入、小区宽带接入、ADSL 宽带接入、CABLE MODEM 宽带接入、ISDN 拨号接入、普通电话拨号接入、GPRS 接入、CDMA 接入等多种因特网接入方式。

(6) VPN 星状互联。由于许多大学有多个校区，且各校区可能有自己的 VPN(或者本校区建不止一个 VPN)，在 VPN 建设中希望能将各 VPN 互联，用户可拨入一 VPN 而共享其他校区资源。

(7) 本地网络和 VPN 网络智能判断。能根据客户端的访问请求，自动选择使用客户本地连接还是使用 VPN 连接。同时，学校有部分资源实际上放在校外，但必须是以该校 IP 地址才能访问。

(8) 连通性要求。VPN 接入用户之间、VPN 接入用户和远程网络中的用户间都可以通过虚拟得到的 IP 地址互相通信。

(9) 应用范围广。可在 VPN 用户与远程局域网之间应用多种业务。如语音、图像和数据库、游戏等应用，也可通过共享等方式访问其他计算机资源。

(10) 符合国家相关法律、标准和安全要求。各 VPN 设备必须符合我国的技术标准和安全标准。

(11) 系统可升级性。可以通过对 VPN 系统升级来适应新的网络应用或是 VPN 上相关协议或标准的升级。

8.8.2 某理工大学校园网 VPN 使用指南

首先登录 VPN 服务网站 http:// melon. dlut. edu. cn/，使用本人学校邮箱(以 @dlut. edu. cn 后缀结尾)用户名及密码，获取当日 VPN 密码。当日该密码只在当天有效，如忘记可到 VPN 服务网站按照上述方法操作，将提示当日密码。第二天(以零点为准)需重新生成当日密码，用新密码连接。登录界面如图 8.5 所示。

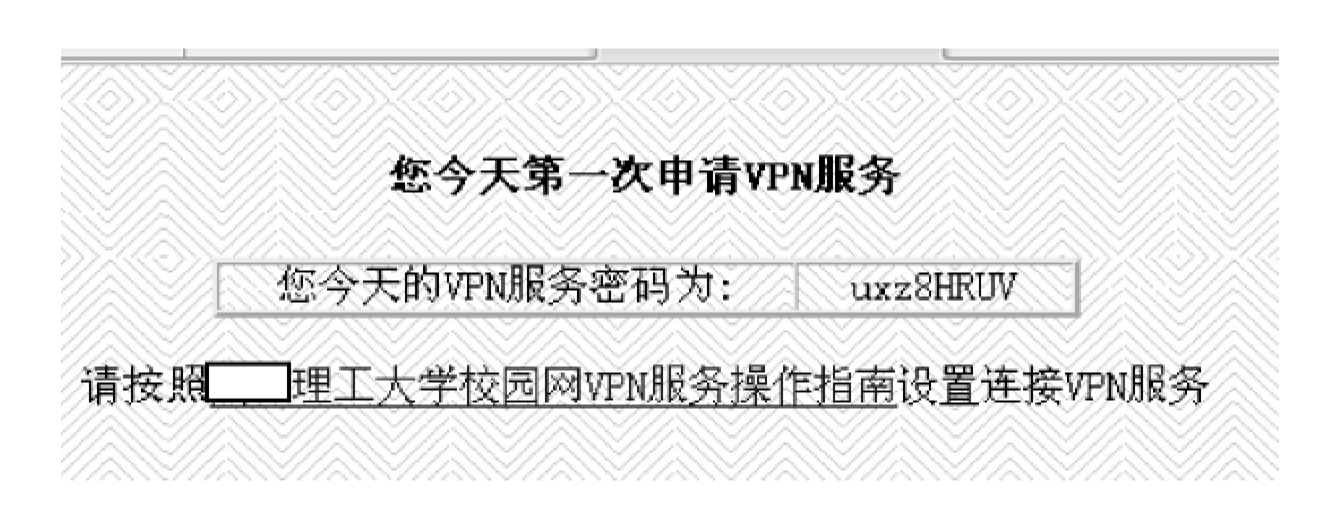


图 8.5　VPN 服务界面

当需要访问校内资源时，就可以使用当日密码，连接校园网 VPN 了。在连接之前要确认自己的主机可以正常接入到 Internet 中，如果主机不能正常上网是无法使用 VPN 的。第一次使用校园网 VPN 需要建立 VPN 连接，方法如下：右击“网上邻居”图标，选择“属性”选项，将打开“网络连接”窗口。在该窗口左侧选择“网络任务”→“创建一个新的连接”命令，启动“新建连接向导”，如图 8.6 所示。



图 8.6　新建连接向导

单击“下一步”按钮，选择网络连接类型，这里需要选择“连接到我的工作场所的网络”，连接到一个商业网络(拨号或者 VPN)，如图 8.7 所示。

单击“下一步”按钮，选择“虚拟专用网络连接”，即使用 VPN 通过 Internet 连接到网络，如图 8.8 所示。

单击“下一步”按钮，要求输入连接名，输入方便自己记忆的名字即可，这里给连接命名为“dlut vpn”。单击“下一步”按钮，设置共用网络，选择“不拨初始连接”，单击“下一步”按

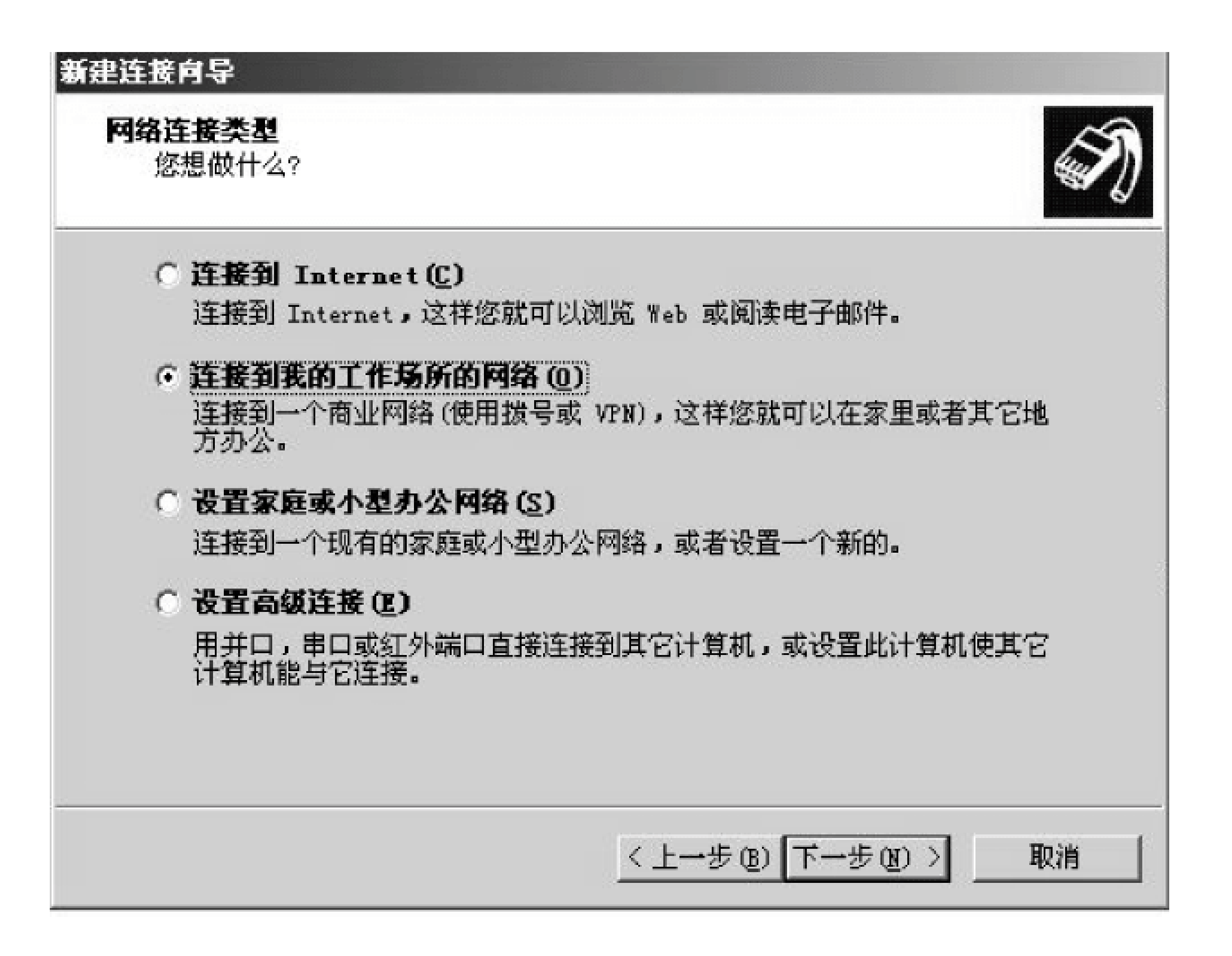


图 8.7　连接到我的工作场所的网络

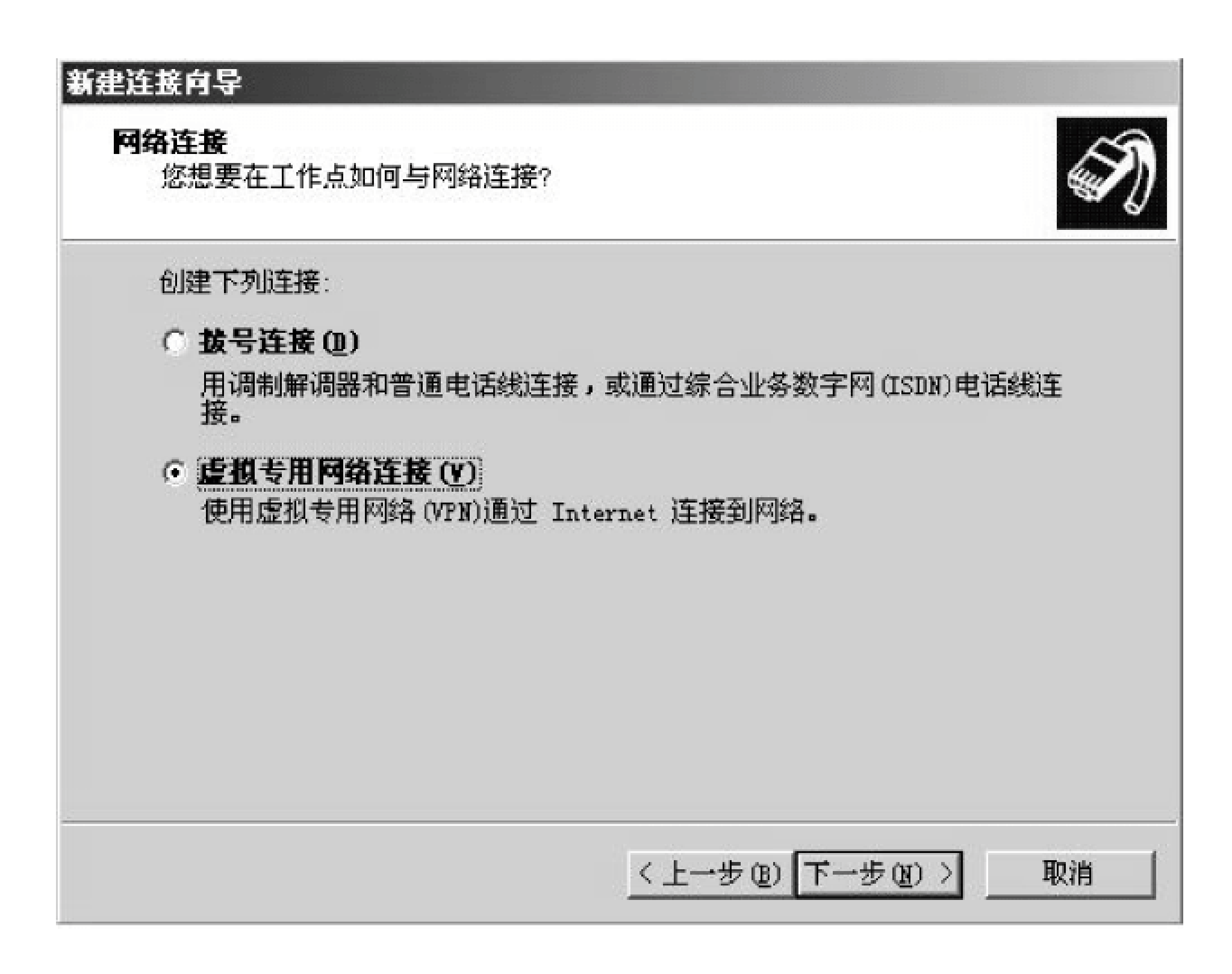


图 8.8　虚拟专用网络连接

钮，输入 VPN 服务器地址，校园网 VPN 服务器的地址为"vpn. dlut. edu. cn"，如图 8.9 所示。

单击"下一步"按钮，显示正在完成新建连接向导，选择"在我的桌面上添加一个到此连接的快捷方式"，然后单击"完成"按钮，这样就完成了 VPN 连接的建立。这时会出现"连接到 dlut vpn"窗口，在此窗口中输入邮箱的用户名和从 VPN 服务网页上获得的当日密码，如图 8.10 所示。然后单击"连接"按钮即可连接到校园网 VPN 服务器，这时就可以访问校内资源。因为每天 VPN 的当日密码都要重新生成，所以不要勾选"为下面的用户保存用户和密码"来保存用户名和密码。

在第一次建立完 VPN 连接后，以后连接不需要再建立连接，只需要双击桌面上的 dlut vpn 快捷键图标，就可以打开连接窗口。或者通过右击选择"网上邻居"→"属性"→"网络连接"窗口，双击其中"虚拟专业网络"下的 dlut vpn 连接，打开连接窗口。然后在连接窗口中输入邮箱用户名和当日密码，就可以再次连接。

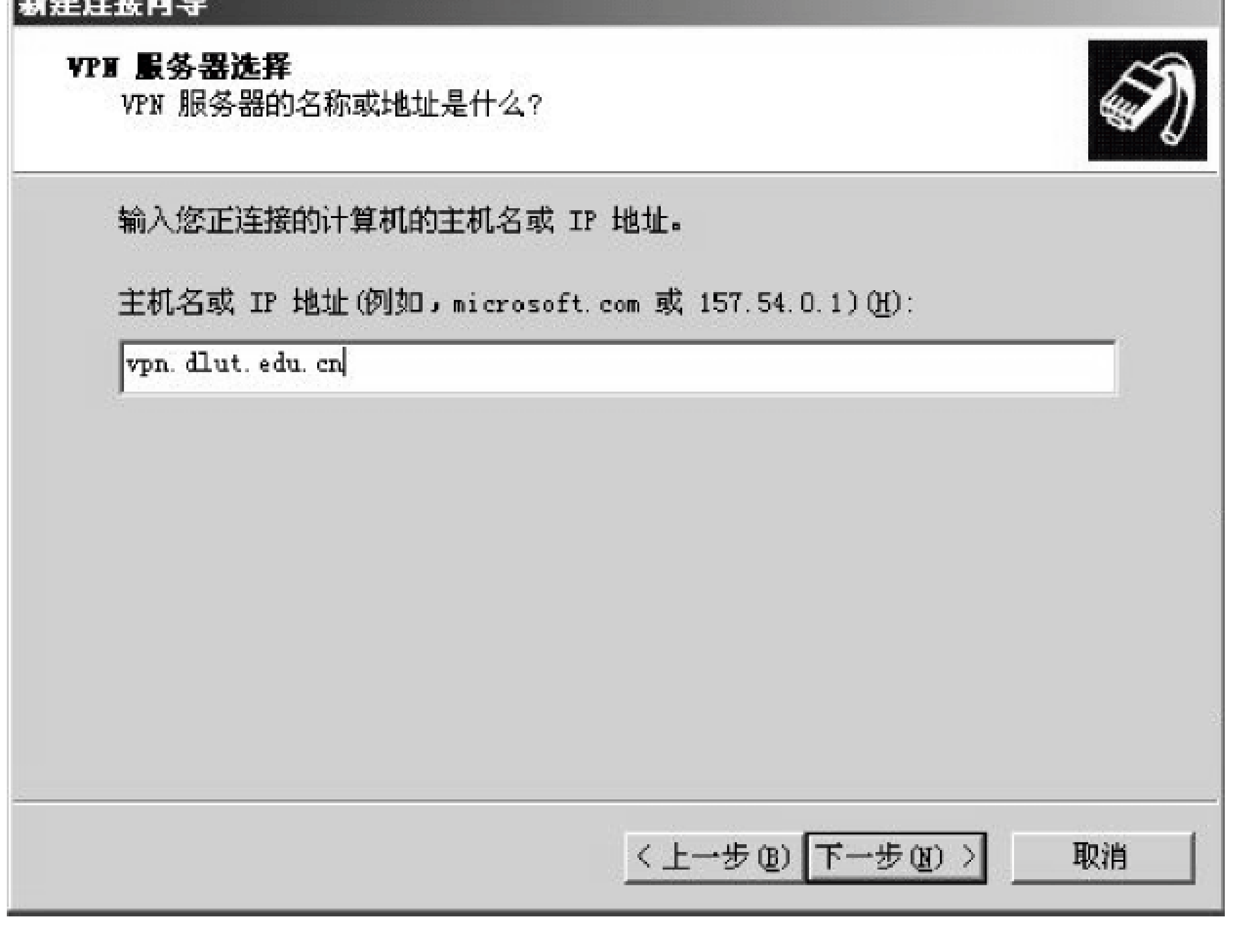



图 8.9　输入 VPN 服务器地址



图 8.10　输入用户和当日密码

当不再访问校园网资源时请双击右下角任务栏中的 dlut vpn 连接,弹出“dlut vpn 状态”窗口,单击“断开”按钮,断开校园网 VPN 的连接。

如果不及时断开,可能会影响其他网络访问。并且由于目前校园网 VPN 负载能力有限,所以对每个用户每天使用的时间限定在 2 小时,不及时断开将一直记录使用时间。如果当天再需要访问校内资源时,可能已经超出了时间限定而无法访问。在 VPN 服务网站生成当日密码处可以查看当日使用时间,当日使用时间超出 2 小时,将无法连接 VPN,请不要再做过多的连接尝试。

课 后 习 题

选择题

1. (　　)协议主要用于加密机制。

A. HTTP　　B. FTP　　C. TELNET　　D. SSL

2. 身份认证的主要目标包括:确保交易者是交易者本人,避免与超过权限的交易者进行交易和(　　)。

A. 可信性　　B. 访问控制　　C. 完整性　　D. 保密性

3. 阻止非法用户进入系统使用(　　)。

A. 病毒防御技术　　B. 数据加密技术

C. 接入控制技术　　D. 数字签名技术

4. HTTPS 是使用以下哪种协议的 HTTP?(　　)。

A. SSL　　B. SSH　　C. Security　　D. TCP

5. 属于第二层的 VPN 隧道协议有(　　)。

A. IPSec　　B. PPTP　　C. GRE　　D. HTTP

填空题

1. (　　)是一种通过使用互联网络的基础设施在网络之间传递数据的方式。

2. 第 2 层隧道协议对应于 OSI 模型的(　　),使用(　　)作为数据交换单位。

3. 第 3 层隧道协议对应于 OSI 模型的(　　),使用(　　)作为数据交换单位。

4. IPSec 隧道模式属于(　　)协议,是将 IP 包封装在附加的 IP 包头中,通过 IP 网络传送。

5. VPN 中密钥的分发有两种方法:一种是通过(　　)方式,另一种采用(　　)动态分发。

6. 认证技术防止数据的(　　)和(　　),它采用一种称为“摘要”的技术。

7. IPSec 安全体系包括 3 个基本协议:(　　)协议为 IP 包提供信息源验证和完整性保证;(　　)协议提供加密机制;(　　)提供双方交流时的共享安全信息。

8. 加解密过程需要两把不同的密钥,一把用来产生数字签名和加密数据,另一把用来验证数字签名和对数据进行解密,这种叫(　　)法。

9. 最常用的两种 hash 函数是(　　)和(　　)。

10. 当一个数据传输通道的两个端点被认为是可信的时候,可以选择(　　)VPN 解决方案。

11. SSL 协议位于(　　)协议与各种(　　)协议之间,为数据通信提供安全支持。

12. (　　)是以安全为目标的 HTTP 通道,简单讲是 HTTP 的安全版。

简答题

1. 什么是虚拟专用网?
2. VPN 的基本功能有哪些?
3. VPN 所需的安全技术有哪些?
4. 通过隧道的建立,可实现哪些功能?
5. IPSec 的安全特性有哪些?
6. IPSec 的好处有哪些?
7. VPN 的分类有哪些?
8. SSL 协议提供的服务主要有哪些?
9. 安全超文本传输协议(HTTPS)的作用是什么?
10. SSL VPN 与 IPSec VPN 安全有哪些?
11. 校园网 VPN 技术要求包括哪些方面?

第 9 章 网络安全解决方案设计

9.1 网络安全方案概念

网络安全方案可以被看做一张施工的图纸，图纸的好坏，直接影响到工程的质量。总的来说，网络安全方案涉及的内容比较多，比较广，比较专业和实际。

对于一名从事网络安全的人来说，网络必须有一个整体和动态的安全概念。对于方案设计者，在整个项目中要有整体把握的能力，不能只关注自己熟悉的某一领域，而对其他领域毫不关心，甚至不理解，这样将写不出好的安全方案。

因为写出来的方案，就是要针对用户所遇到的问题，用已知的产品和技术去解决，设计人员只有对安全技术有很深的了解，对网络产品有全面的接触，设计出来的安全方案才能更加接近用户的实用要求。

9.2 评价网络安全方案的质量

一份网络安全方案需要从以下 8 个方面来把握：

(1) 体现唯一性。由于安全的复杂和特殊，唯一性是评估安全方案最重要的一个标准。实际中，每一个特定网络都是唯一的，需要根据实际情况来处理。

(2) 对安全技术和安全风险有一个综合把握和理解，包括现在和将来可能出现的所有情况。

(3) 对用户的网络系统可能遇到的安全风险和安全威胁，结合现有的安全技术和安全风险，要有一个合适、中肯的评估，不能夸大，也不能缩小。

(4) 对症下药。用相应的安全产品、安全技术和管理手段，降低用户网络系统当前可能遇到的风险和威胁，消除风险和威胁的根源，增强整个网络系统抵抗风险和威胁的能力，增强系统本身的免疫力。

(5) 方案中要体现出对用户的服务支持，这是很重要的一部分。因为产品和技术都将体现在服务中，用服务来保证质量和提高质量。

(6) 在设计方案时，要明白网络系统安全是一个动态的、整体的和专业的工程，不能一步到位解决用户所有的问题。

(7) 方案出来后，要不断和用户进行沟通，能够及时得到他们对网络系统在安全方面的要求、期望和所遇到的问题。

(8) 方案中所涉及的产品和技术都要经得起验证、推敲和实施，既要有理论根据，也要有实际基础。

9.3 网络安全方案的框架

总体上说，一份安全解决方案的框架涉及概要安全风险分析、实际安全风险分析、网络系统的安全原则、安全产品、风险评估和安全服务 6 大方面，可以根据用户的实际需求取舍其中的某些方面。

9.4 网络安全需求分析

网络安全的唯一性和动态性决定了不同的网络需要有不同的解决方案。下面通过一个实际的案例，来提高对安全方案设计的理解。

项目名称：腾飞科技集团公司(公司名为虚构)网络信息系统的安全方案建议书。

9.4.1 项目要求

腾飞科技集团在网络安全方面提出以下 5 个方面的要求。

(1) 安全性。全面有效地保护企业网络系统的安全，保护计算机硬件、软件、数据、网络不因偶然的或恶意破坏等原因遭到更改、泄露和丢失，确保数据的完整性。

(2) 可控性和可管理性。可自动和手动分析网络安全状况，适时检测并及时发现记录潜在的安全威胁，制定安全策略，及时报警、阻断不良攻击行为，具有很强的可控性和可管理性。

(3) 系统的可用性。在某部分系统出现问题时，不影响企业信息系统的正常运行，具有很强的可用性和及时恢复性。

(4) 可持续发展。满足腾飞科技集团公司业务需求和企业可持续发展的要求，具有很强的可扩展性和柔韧性。

(5) 合法性。所采用的安全设备和技术具有我国安全产品管理部门的合法认证。

9.4.2 工作任务

该网络安全项目的工作任务在于以下 4 个方面：

(1) 研究该公司的计算机网络系统(包括各级机构、基层生产单位和移动用户的广域网)的运行情况(包括网络结构、性能、信息点数量、采取的安全措施等)，对网络面临的威胁以及可能承担的风险进行定性与定量的分析评估。

(2) 研究该公司的计算机操作系统(包括服务器操作系统、客户端操作系统等)的运行情况(包括操作系统的版本、提供的用户权限分配策略等)，在操作系统最新发展趋势的基础上，对操作系统本身的缺陷以及可能承担的风险进行定性和定量的分析和评估。

(3) 研究该公司的计算机应用系统(包括信息管理系统、办公自动化系统、Internet/intranet 信息发布系统等)的运行情况(包括应用体系结构、开发工具、数据库软件和用户权限分配策略等)，在满足各级管理人员、业务操作人员的业务需求的基础上，对应用系统存在的问题、面临的威胁以及可能承担的风险进行定性与定量的分析和评估。

(4) 根据以上的定性和定量的评估,结合用户需求和国内外网络安全最新发展趋势,有针对地制定该公司计算机网络系统的安全策略和解决方案,确保该公司计算机网络信息系统安全、可靠地运行。

9.5 解决方案设计

深度网络安全公司(公司名为虚构)通过竞标,以 500 万的工程造价得到了该项目的实施权。在解决方案设计中需要包含以下 9 个方面的内容:

(1) 施工方公司背景简介;

(2) 集团的安全风险分析;

(3) 完整网络安全实施方案的设计;

(4) 实施方案计划;

(5) 技术支持和服务承诺;

(6) 产品报价;

(7) 产品介绍;

(8) 第三方检测报告;

(9) 安全技术培训。

9.5.1 施工方公司背景简介

介绍深度网络安全公司的背景,需要包括:公司简介、公司人员结构、曾经成功的案例、产品或者服务的许可证或认证、被施工方腾飞科技集团实施网络安全方案的意义。

9.5.2 安全风险分析

对现有网络物理结构的安全分析。详细分析腾飞科技集团公司与各分公司的网络结构,包括内部网、外部网和远程网。

对网络系统的安全分析。详细分析腾飞科技集团公司与各分公司的网络的实际连接、Internet 的访问情况、桌面系统的使用情况和主机系统的使用情况,找出可能存在的安全风险。

对网络应用的安全分析。详细分析腾飞科技集团公司与各分公司的所有服务系统以及应用系统,找出可能存在的安全风险。

9.5.3 解决方案

解决方案包括以下 5 个方面:

(1) 建立腾飞科技集团公司系统信息安全体系结构框架;

(2) 技术实施策略;

(3) 安全管理工具;

(4) 紧急响应;

(5) 灾难恢复。

9.5.4 实施方案

实施方案包括项目管理以及项目质量保证。

9.5.5 技术支持和服务承诺

包括技术支持的内容和技术支持的方式。

(1) 技术支持的内容包括:

① 安装调试项目中所涉及的全部产品和技术;

② 安全产品以及技术文档;

③ 提供安全产品和技术的最新信息;

④ 服务器内产品免费升级。

(2) 安全项目完成以后提供的技术支持服务方式包括:

① 客户现场 24 小时支持服务;

② 客户支持中心热线电话;

③ 客户支持中心 E-mail 服务;

④ 客户支持中心 Web 服务。

9.5.6 产品报价

项目所涉及全部产品和服务的报价列表。

9.5.7 产品介绍

腾飞科技集团公司安全项目中所有涉及的产品介绍,主要是使用户清楚所选择的产品是什么,不用很详细,但要描述清楚。

9.5.8 第三方检测报告

由一个第三方的中立机构,对实施好的网络安全构架进行安全扫描与安全检测,并提供相关的检测报告以备存档。

9.5.9 安全技术培训

安全技术培训包括:

(1) 管理人员的安全培训;

(2) 安全技术基础培训;

(3) 安全攻防技术培训;

(4) Windows XP/NT/2000/2003 的系统安全管理培训;

(5) 安全产品的培训。

具体的网络安全设计方案,详见附录 A。

课 后 习 题

简答题

1．网络安全方案需要从哪几个方面来把握？

2．一份安全解决方案的框架涉及哪几个大方面？

3．企业在网络安全方面一般会提出哪几方面的要求？

4．网络安全方案项目的工作任务是什么？

5．解决方案设计中需要包含哪几个方面的内容？

6．技术支持方式有哪些形式？

7．安全技术培训一般有哪些内容？

第10章　实验1　Sniffer 软件的使用

10.1　实验目的及要求

10.1.1　实验目的

通过实验操作掌握 Sniffer 软件的安装与基本功能的使用，对于监控软件原理有一定的了解，能够熟练使用 Sniffer 软件实现常用的监控功能。

10.1.2　实验要求

根据第 2 章介绍的 Sniffer 软件的功能和步骤来完成实验，在掌握基本功能的基础上，实现日常监控应用，给出实验总结报告。

10.1.3　实验设备及软件

2 台磁盘格式配置为 NTFS 的 Windows 2000/XP 操作系统的计算机，局域网环境、FTP 服务器、Sniffer Pro 4.7.5 软件。

10.1.4　实验拓扑

实验的拓扑结构如图 10.1 所示。

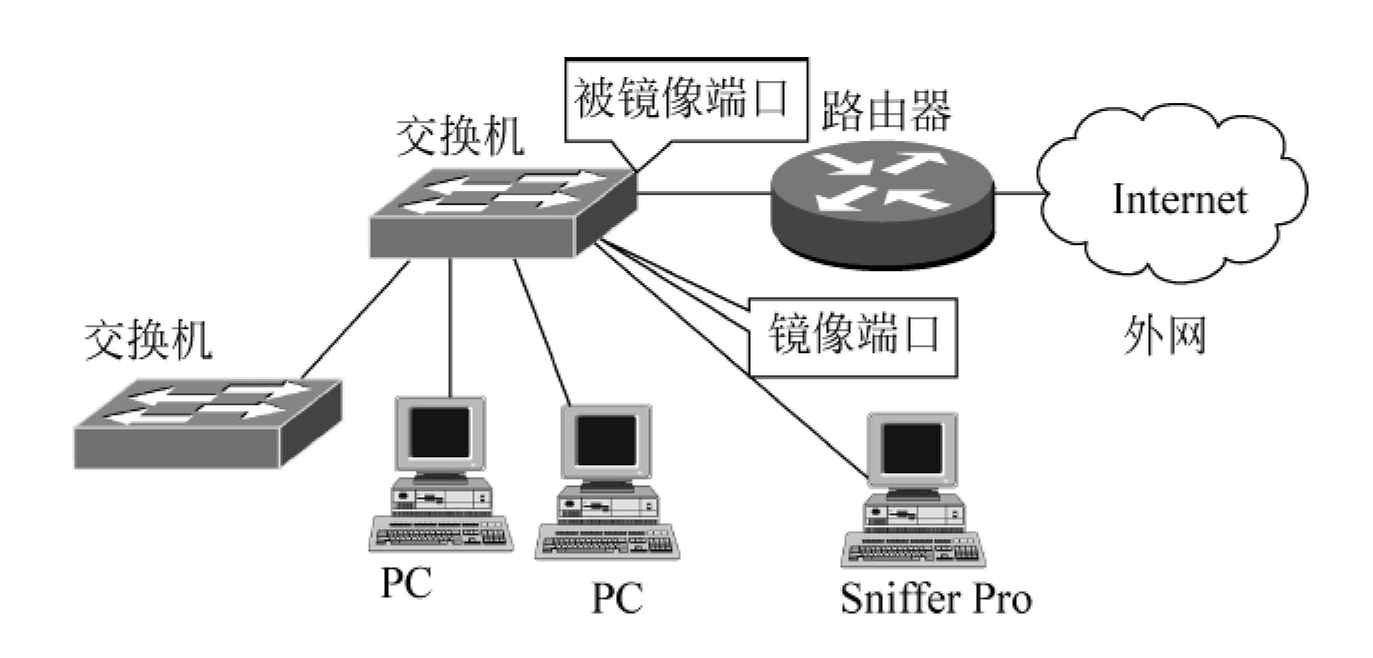


图 10.1　实验拓扑

10.1.5　交换机端口镜像配置

以锐捷交换机为例，fa0/2 端口监控 fa0/10 端口的配置如下所示：

```
Switch >en
Switch #conf t     ! 进入全局配置模式
```

```
Switch(config)# monitor session 1 source interface fastEthernet 0/10 both
! 设置被监控口
Switch(config)# monitor session 1 destination interface fastEthernet 0/2
! 设置监控口
Switch(config)# end
Switch# wr
Switch# show monitor session 1 ! 查看当前配置
Switch(config)# no monitor session 1 ! 清除当前配置
```

10.2 Sniffer 软件概述

Sniffer Pro 软件是 NAI 公司推出的功能强大的协议分析软件。本实验利用 Sniffer Pro 软件的强大功能,解决网络中的一系列故障问题。

10.2.1 功能简介

下面给出了 Sniffer 软件的一部分功能介绍,更多功能的详细介绍可以参考 Sniffer Pro 软件的在线帮助。

(1) 捕获网络流量进行详细分析;

(2) 利用专家分析系统诊断问题;

(3) 实时监控网络活动;

(4) 收集网络利用率和错误。

Sniffer 的安装非常简单,执行 setup 安装程序后连续单击"确定"按钮即可。第一次运行时需要选择网卡,确定从计算机的哪个网卡上接收数据。菜单中选择"文件"→"选定设置",如图 10.2 所示。

选择网卡后才能正常工作。该软件如果安装在 Windows 98 操作系统上,Sniffer 可以选择拨号适配器对窄带拨号进行操作。如果安装了 EnterNet500 等 PPPOE 软件,还可以选择虚拟出的 PPPOE 网卡。对于安装在 Windows 2000/XP 上则无上述功能,这和操作系统有关。

图 10.3 给出了 Sniffer Pro 中快捷键的位置。



图 10.2 选择捕获网卡



图 10.3 快捷键

10.2.2 报文捕获解析

1. 捕获面板

报文捕获功能可以在报文捕获面板中进行设置，如图 10.3 所示。按钮的功能从左到右分别为：捕获开始、捕获暂停、捕获停止、停止并显示、显示、定义过滤器、选择过滤器等。

2. 捕获过程报文统计

在捕获过程中可以通过捕获面板查看捕获报文的数量和缓冲区的利用率，如图 10.4 所示。

3. 捕获报文查看

Sniffer Pro 提供了强大的分析能力和解码功能。如图 10.5 所示，对于捕获的报文提供了一个专家分析系统进行查看分析，还有解码选项及图形和表格的统计信息。

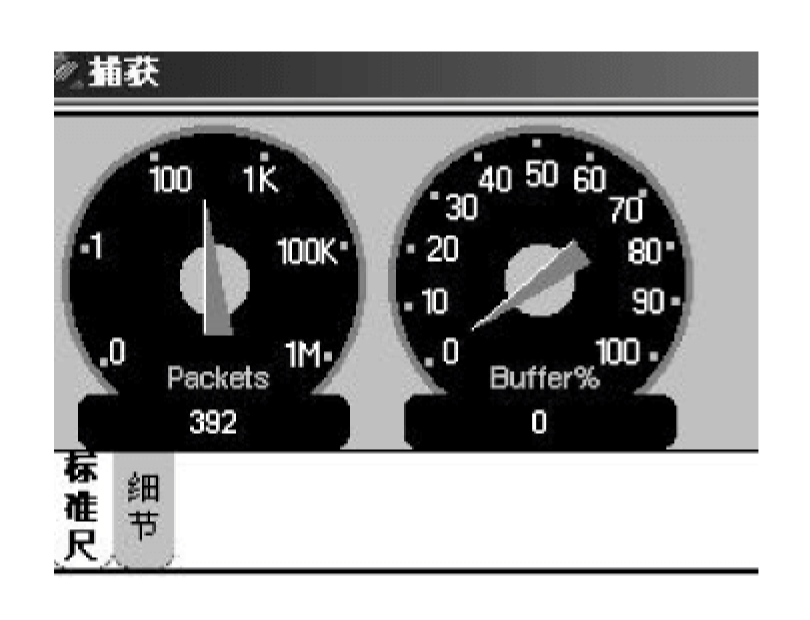


图 10.4　捕获过程报文统计面板

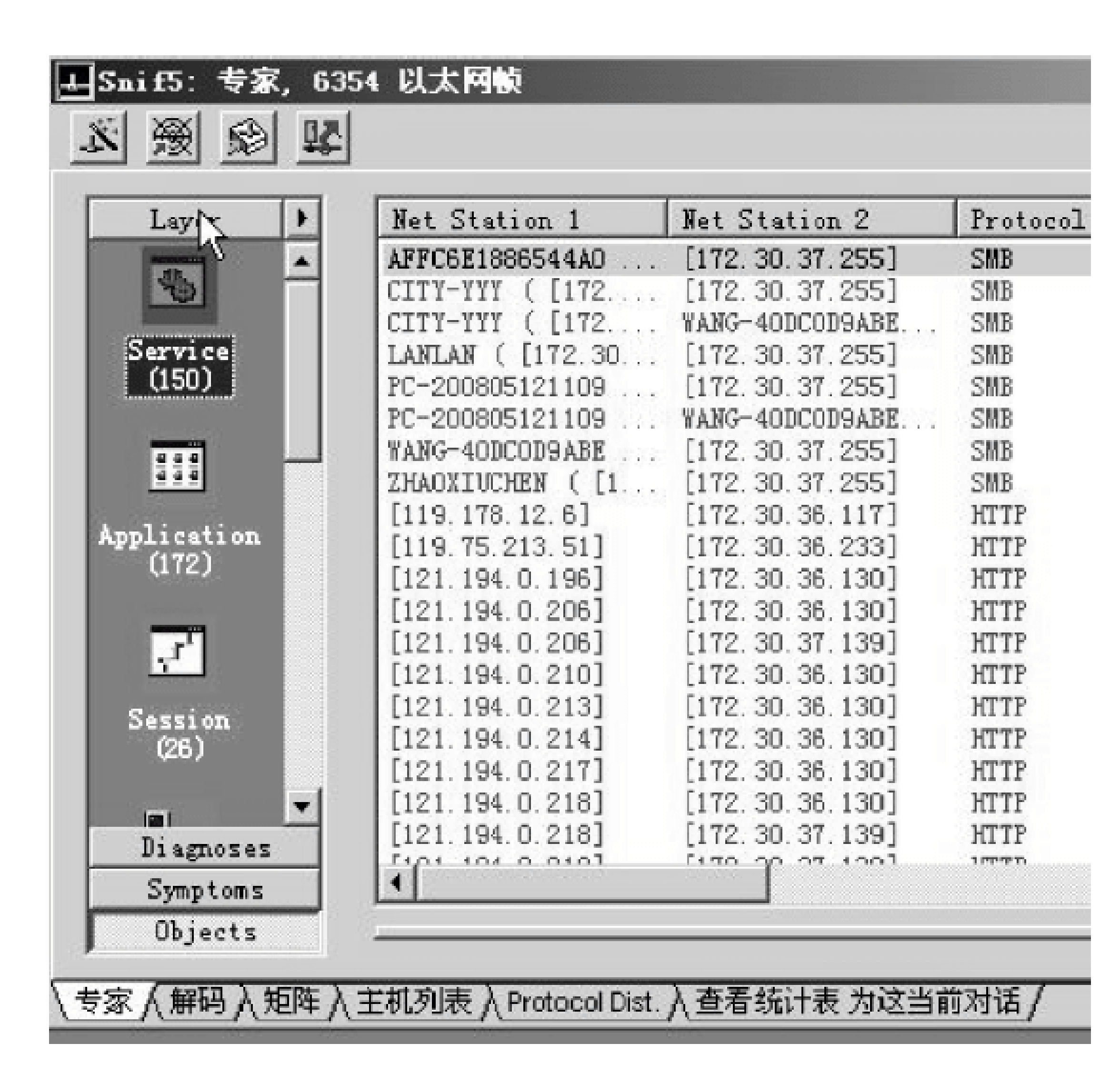


图 10.5　专家分析系统

4. 专家分析

专家分析系统提供了一个分析平台，对网络上的流量进行了一些分析，对于分析出的诊断结果可以通过查看在线帮助获得。

在图 10.6 中，显示出了在网络中 WINS 查询失败的次数及 TCP 重传的次数统计等内容，可以方便了解网络中高层协议出现故障的可能点。

对于某项统计分析可以通过用鼠标双击此条记录来查看其详细信息，也可以对详细信息中的每一项做进一步查看。

5. 解码分析

图 10.7 是对捕获报文进行解码的显示，通常分为三部分，目前大部分此类软件结构都采用这种结构显示。对于解码主要要求分析人员对协议比较熟悉，这样才能看懂解析出来的报文。使用该软件是很简单的事情，要能够利用软件解码分析来解决问题的关键，要对各种层次的协议了解的比较透彻。工具软件仅能提供一个辅助分析的手段。

对于 MAC 地址，Sniffer Pro 进行了头部的替换，如 00e0fc 开头的就替换成 Huawei，这样有利于了解网络上各种相关设备的制造厂商信息。

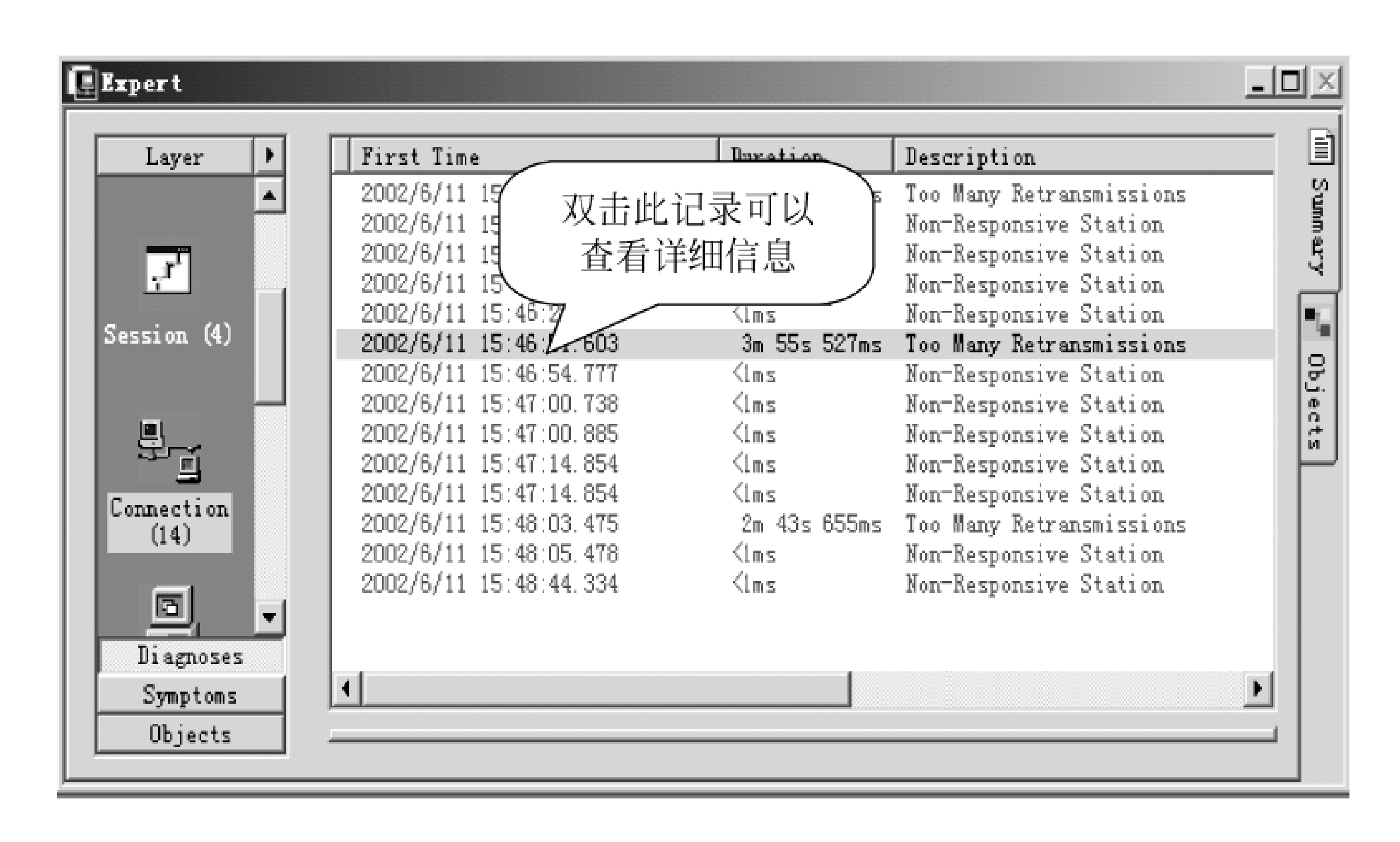


图 10.6　分析出的结果

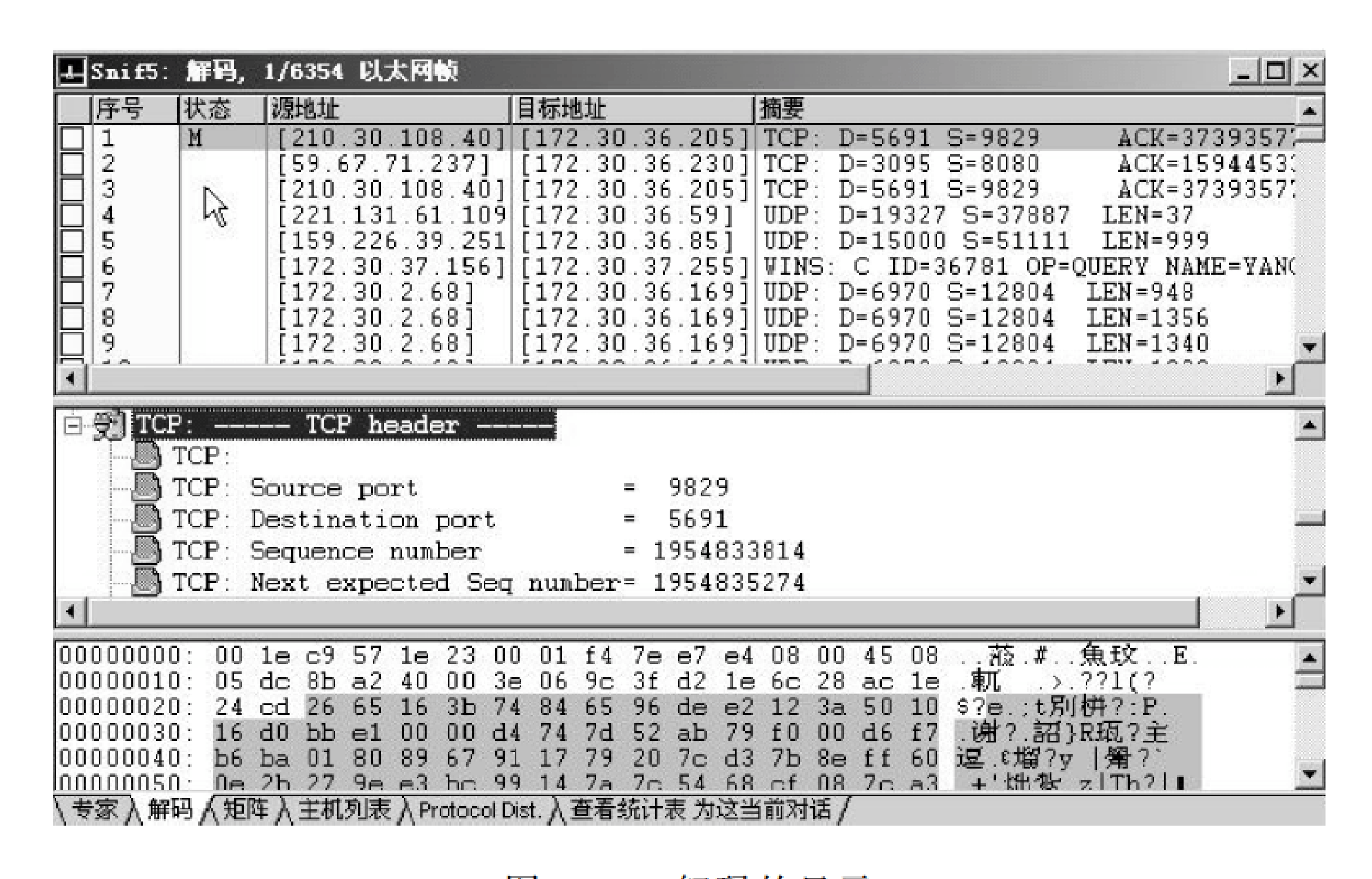


图 10.7　解码的显示

功能是按照过滤器设置的过滤规则进行数据的捕获或显示。在菜单上的位置分别为“捕获”→“定义过滤器和显示”→“定义过滤器”。

过滤器可以根据物理地址、IP 地址和协议的选择进行组合筛选。

统计分析功能是对于矩阵、主机列表、协议分类、统计表等提供了丰富的组合统计，操作起来比较简单，可以很快掌握，这里不再详细介绍。

10.2.3　设置捕获条件

1. 基本捕获条件

基本的捕获条件有两种：

(1) 链路层捕获，按源 MAC 和目的 MAC 地址进行捕获，输入方式为十六进制连续输入，如 00E0FC123456，参见图 10.8。

(2) IP 层捕获，按源 IP 和目的 IP 进行捕获。输入方式为点间隔方式，如 10.107.1.1。如果选择 IP 层捕获条件则 ARP 等报文将被过滤掉。

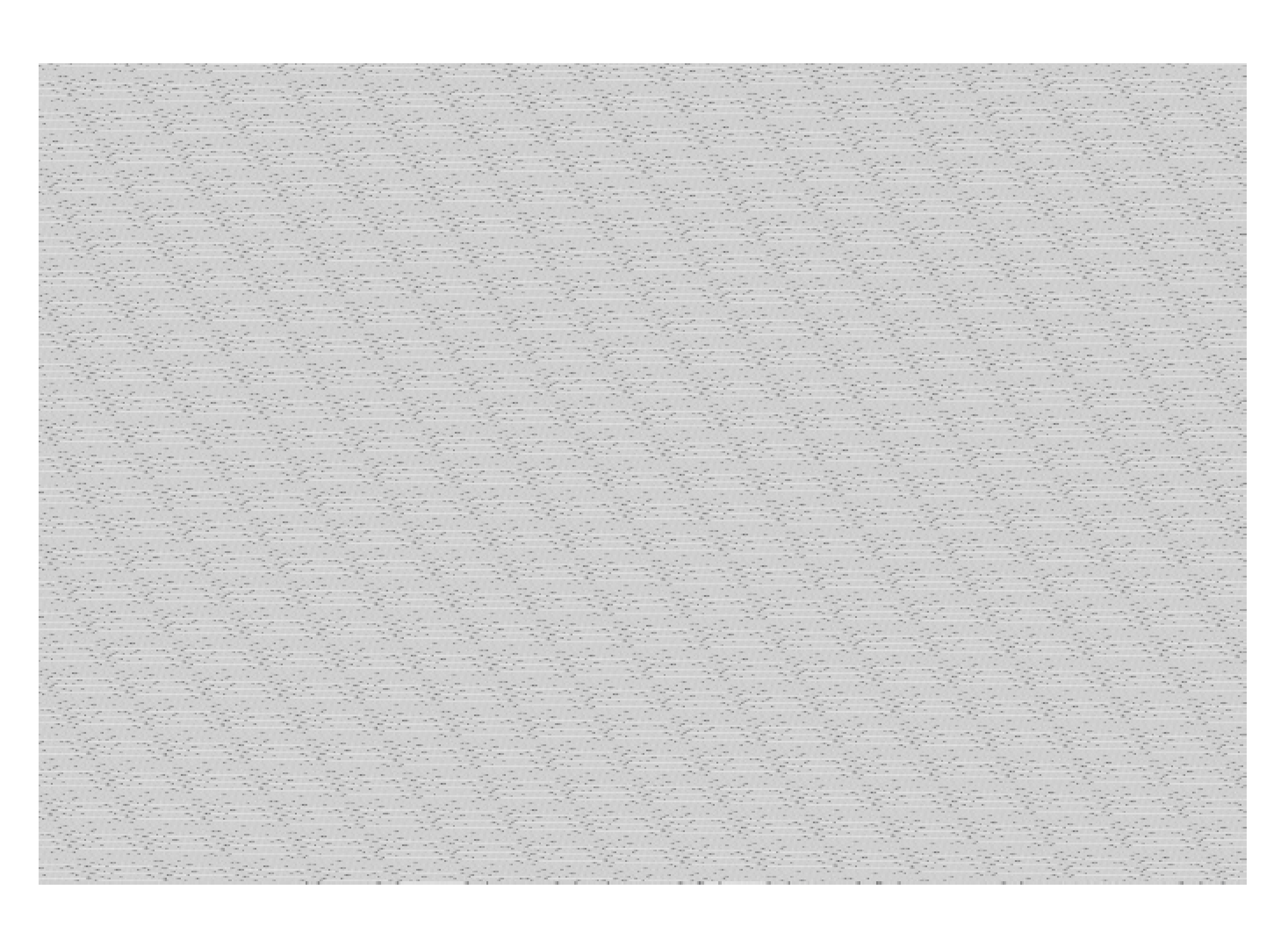


图 10.8　设置捕获条件

2. 高级捕获条件

在“高级”选项卡下,可以编辑协议捕获条件,如图 10.9 所示。

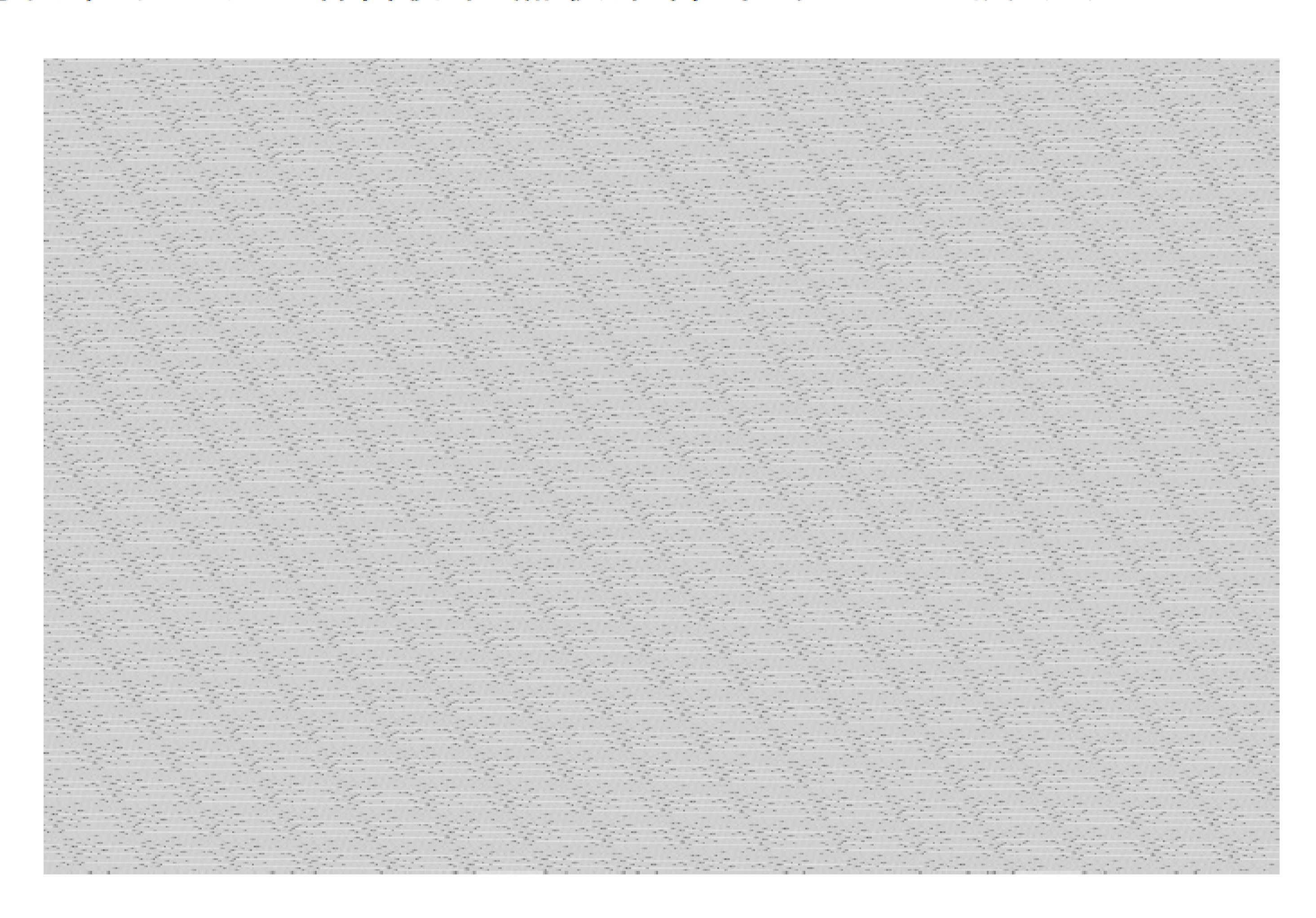


图 10.9　设置高级捕获条件

在协议选择树中可以选择需要捕获的协议条件,如果什么都不选,则表示忽略该条件,捕获所有协议。

在“数据包大小”条件下,可以选择捕获等于、小于、大于某个值的报文。

在“数据包类型”条件下,可以选择捕获网络上那些种类的数据包。

单击“配置文件”按钮,可以将当前设置的过滤规则进行保存,然后在捕获主面板中,即可选择保存的捕获条件。

3. 任意捕获条件

在“数据模式”选项卡下,可以编辑任意捕获条件,如图 10.10 所示。

用这种方法可以实现复杂的报文过滤,但很多时候是得不偿失,有时截获的报文本来就不多,还不如自己看看来得快。



图 10.10　编辑任意捕获条件

10.2.4　网络监视功能

网络监视功能能够时刻监视网络统计，网络上资源的利用率，并能够监视网络流量的异常状况，这里只介绍仪表盘和应用响应时间，直接使用即可，比较简单。

1. 仪表盘

仪表盘可以监控网络的利用率、流量及错误报文等内容。通过应用软件可以清楚看到此功能，如图 10.11 所示。

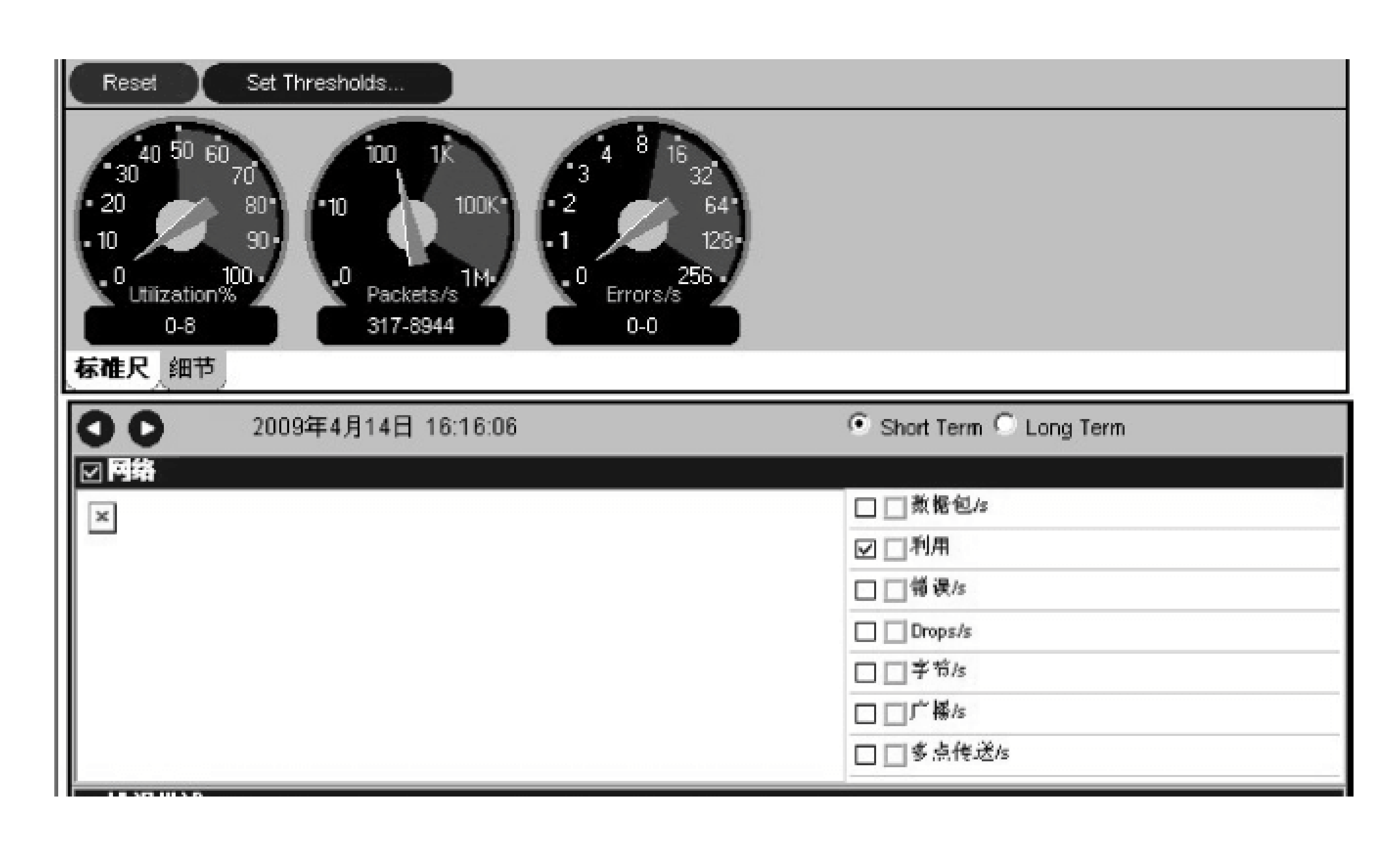


图 10.11　仪表盘界面

2. 应用响应时间

应用响应时间(ART)是可以监视 TCP/UDP 应用层程序在客户端和服务器响应时间，如 HTTP、FTP、DNS 等应用，如图 10.12 所示。

服务器地址	客户地址	AvgRsp	90%Rsp	MinRsp	MaxRsp	TotRsp	0-25	26-50
119.75.213.50	PC-200811211103	17	15	16	19	4	4	0
125.46.1.226	PC-200811211103	128	126	127	129	2	0	0
202.108.23.61	PC-200811211103	115	118	113	120	6	0	0
202.112.28.153	PC-200811211103	42	46	37	49	78	0	78
202.116.160.92	PC-200811211103	50	54	48	55	124	0	49
222.73.207.132	PC-200811211103	319	323	296	337	4	0	0
222.73.207.136	PC-200811211103	285	279	281	288	2	0	0
60.28.22.61	PC-200811211103	140	136	140	140	2	0	0
74.125.153.100	PC-200811211103	81	87	75	92	5	0	0

图 10.12　ART 界面

10.3　数据报文解码详解

本节主要对数据报文分层、以太报文结构、IP 协议解码分析做简单的描述，目的在于介绍 Sniffer Pro 在协议分析中的功能作用并通过解码分析对协议进一步了解。

10.3.1　数据报文分层

如图 10.13 所示，对于 4 层网络结构，其不同层次完成不同功能，每一层次由众多协议组成。

如图 10.14 所示，在 Sniffer Pro 的解码表中分别对每一个层次协议进行解码分析。链路层对应 DLC；网络层对应 IP；传输层对应 UDP；应用层对应的是 NETB 等高层协议。Sniffer 可以针对众多协议进行详细结构化解码分析，并利用树状结构良好地表现出来。

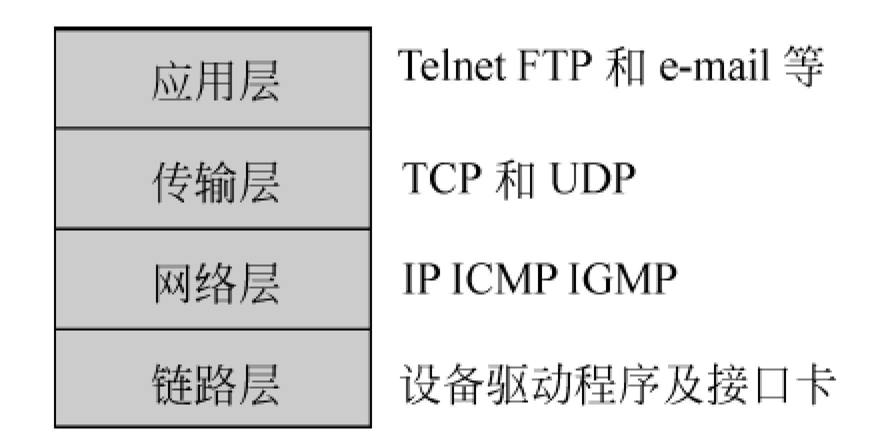


图 10.13　4 层网络结构图

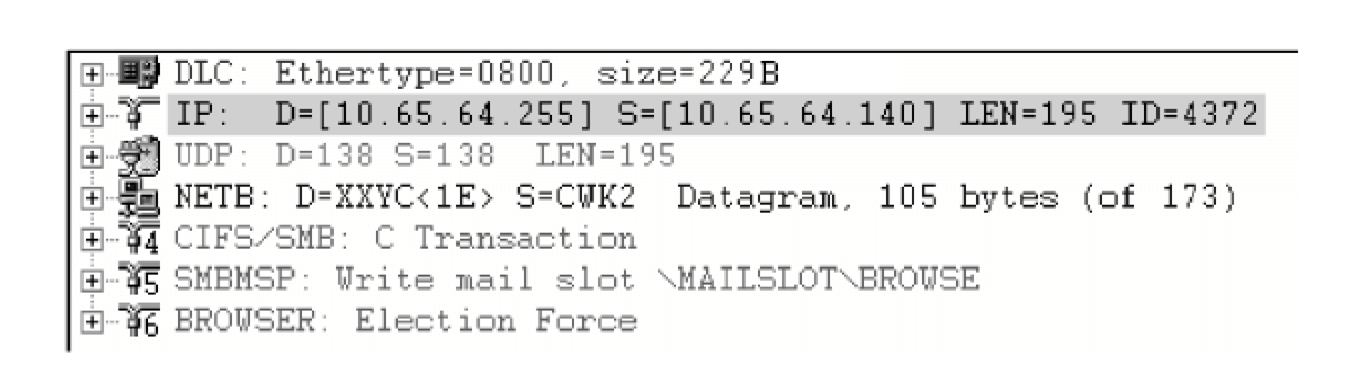


图 10.14　分层协议解码分析

10.3.2　以太网帧结构

如图 10.15 所示，Ethernet Ⅱ 以太网帧类型报文结构为：目的 MAC 地址(6B)＋源 MAC 地址＋(6B)上层协议类型(2B)＋数据字段(46～1500B)＋校验(4B)。图 10.16 为以太网帧结构的显示。



图 10.15　以太网帧结构

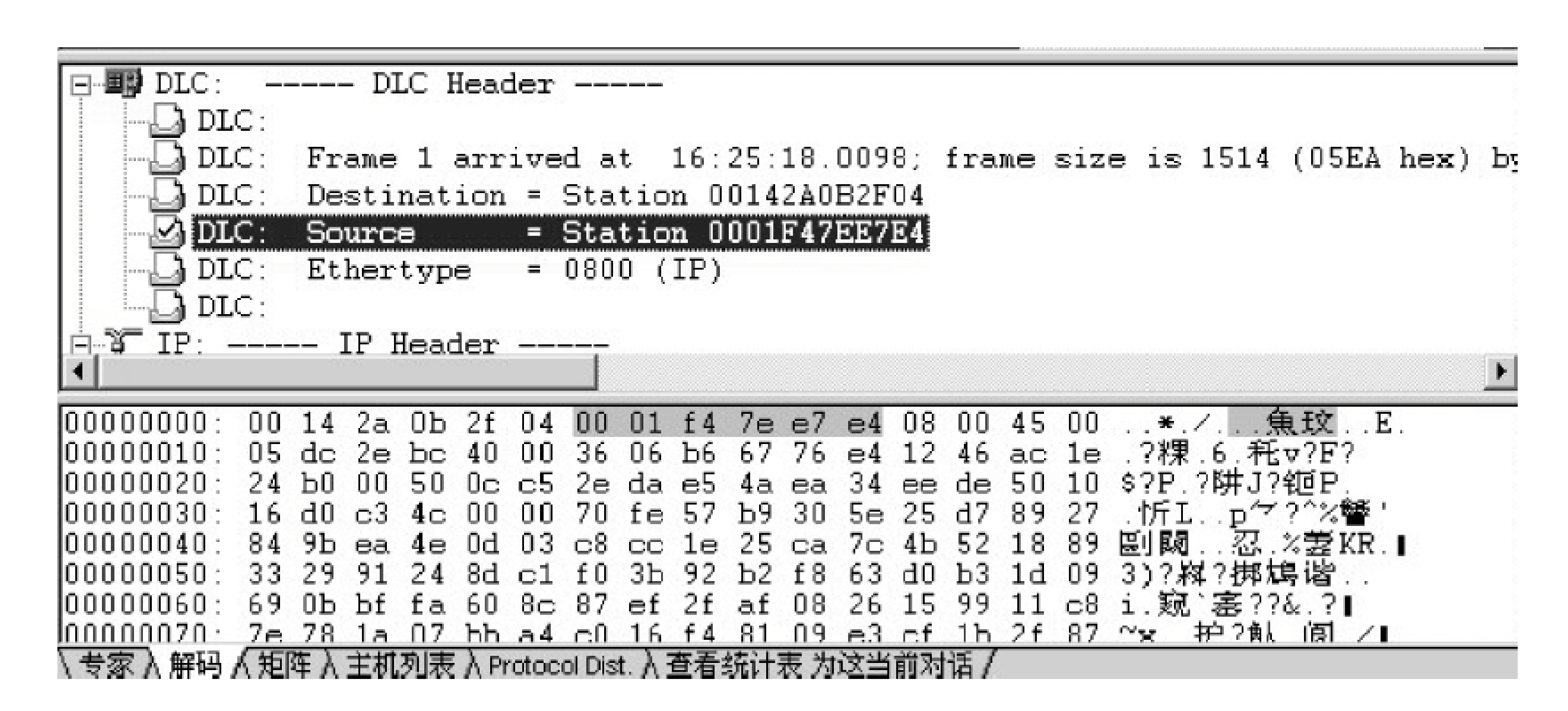


图 10.16　以太网帧结构的显示

Sniffer Pro 会在捕获报文的时候自动记录捕获的时间，在解码显示时显示出来，在分析问题时提供了很好的时间记录。

源目的 MAC 地址在解码框中可以将前 3 个字节代表厂商的字段翻译出来，方便定位问题。例如，网络上 2 台设备 IP 地址设置冲突，可以通过解码翻译出厂商信息方便的将故障设备找到，如 00e0fc 为华为，010042 为 Cisco 等。如果需要查看详细的 MAC 地址，可在解码框中单击此 MAC 地址，在下面的表格中会突出显示该地址的十六进制编码。

对于 IP 网络来说，Ethertype 字段承载的是上层协议的类型，主要包括 0x800（IP 协议）、0x806（ARP 协议）。

IEEE 802.3 以太网报文结构如图 10.17 所示。

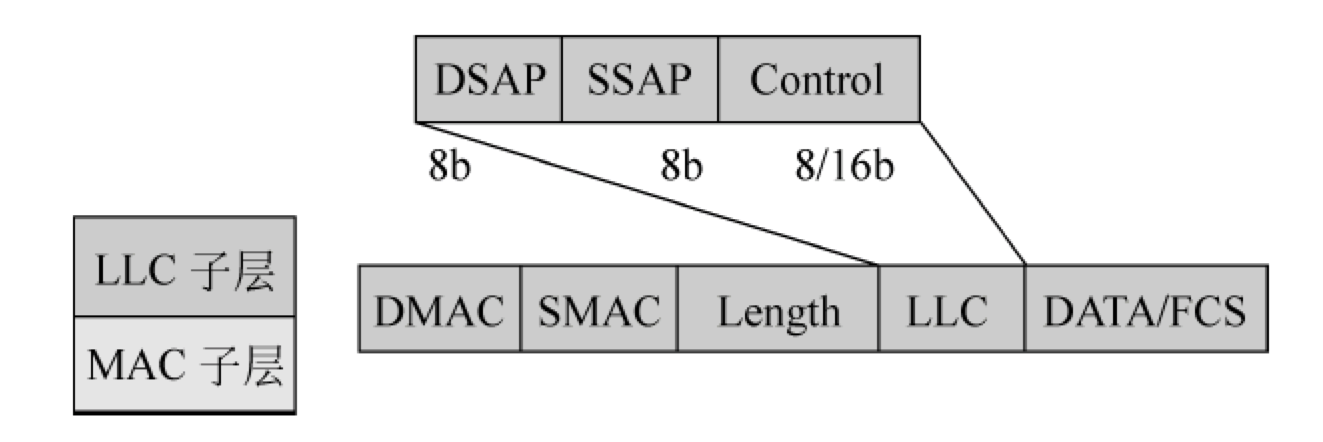


图 10.17　IEEE 802.3 以太网帧结构

图 10.18 为 IEEE 802.3SNAP 帧结构，与 Ethernet Ⅱ不同的是目的和源地址后面的字段代表的不是上层协议类型而是报文长度，并多了 LLC 子层。

```
DLC:  ----- DLC Header -----
  DLC:
  DLC:  Frame 1 arrived at  12:13:38.8809; frame size is 64 (0040 hex)
  DLC:  Destination = Multicast 0180C2000000, Bridge_Group_Addr
  DLC:  Source      = Station Cisco EC9C54
  DLC:  802.3 length = 38
  DLC:
LLC:  ----- LLC Header -----
  LLC:
  LLC:  DSAP Address = 42, DSAP IG Bit = 00 (Individual Address)
  LLC:  SSAP Address = 42, SSAP CR Bit = 00 (Command)
  LLC:  Unnumbered frame: UI
  LLC:
```

图 10.18　IEEE 802.3SNAP 帧结构

10.3.3　IP 协议

IP 报文结构为 IP 协议头＋载荷。其中，对 IP 协议头部的分析是分析 IP 报文的主要内容之一。关于 IP 报文详细信息请参考相关资料。这里给出了 IP 协议首部的一个结构，参见图 10.19。

- 版本：4——IPv4
- 首部长度：单位为 4 字节，最大 60 字节
- TOS：IP 优先级字段
- 总长度：单位字节，最大 65 535 字节
- 标识：IP 报文标识字段
- 标志：占 3 比特，只用到低位的两个比特

  MF(More Fragment)

  MF＝1，后面还有分片的数据包

```
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 B
IP: Type of service = 00
IP:        000. ....    = routine
IP:        ...0 ....  = normal delay
IP:        .... 0...  = normal throughput
IP:        .... .0..  = normal reliability
IP:        .... ..0.  = ECT bit - transport protocol
IP:        .... ...0  = CE bit - no congestion
IP: Total length     = 1500 B
IP: Identification   = 11964
IP: Flags            = 4X
IP:        .1.. ....  = don't fragment
IP:        ..0. ....  = last fragment
IP: Fragment offset  = 0 B
IP: Time to live     = 54 seconds/hops
IP: Protocol         = 6 (TCP)
IP: Header checksum  = B667 (correct)
IP: Source address       = [118.228.18.70]
IP: Destination address  = [172.30.36.176]
IP: No options
IP:
```

图 10.19　IP 协议首部的解码分析结构

MF=0,分片数据包的最后一个

DF(Don't Fragment)

DF=1,不允许分片

DF=0,允许分片

- 段偏移:分片后的分组在原分组中的相对位置,总共 13 比特,单位为 8 字节
- 寿命:TTL(Time To Live)丢弃 TTL=0 的报文
- 协议:携带的是何种协议报文

  1 :ICMP

  6 :TCP

  17:UDP

  89:OSPF
- 头部检验和:对 IP 协议首部的校验和
- 源 IP 地址:IP 报文的源地址
- 目的 IP 地址:IP 报文的目的地址

图 10.19 为 Sniffer Pro 对 IP 协议首部的解码分析结构,和 IP 首部各个字段相对应,并给出了各个字段值所表示含义的英文解释。报文协议(Protocol)字段的编码为 6,代表 TCP 协议,其他字段的解码含义可以与此类似。只要对协议理解的比较清楚,对解码内容的理解将会变得很容易。

10.4　使用 Sniffer Pro 监控网络流量

10.4.1　设置地址簿

如何查询网关流量是最为常用、重要的查询之一。

扫描 IP-MAC 对应关系。这样做是为了在查询流量时,能方便判断具体流量终端的位置。MAC 地址不如 IP 地址方便。

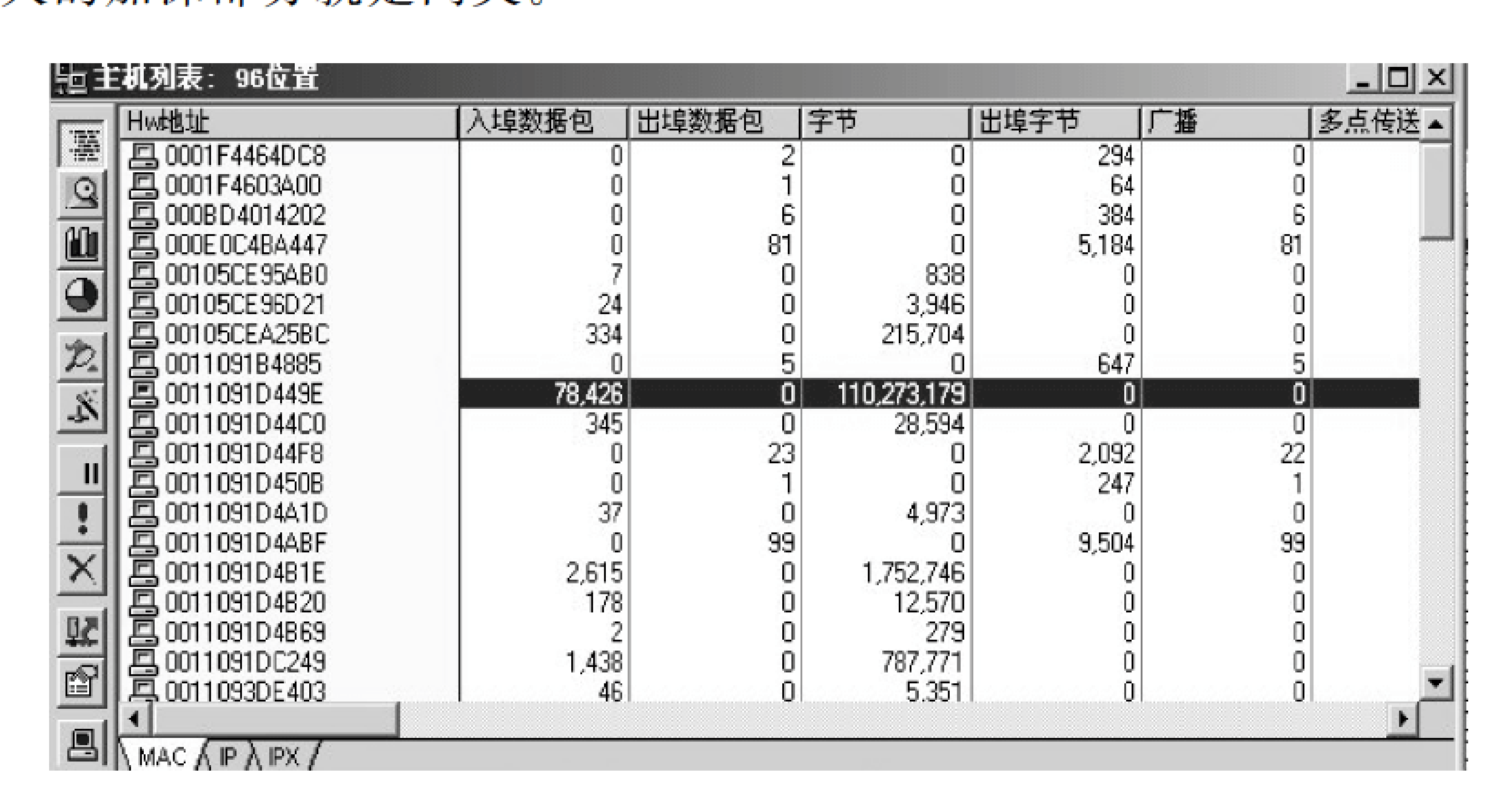
选择菜单栏中的“工具”→“地址簿”，单击左边的放大镜(autodiscovery 扫描)按钮，在弹出的窗口中输入所要扫描的 IP 地址段，本例输入 172.30.37.1-172.30.37.255。单击“好”按钮，如图 10.20 所示，系统会自动扫描 IP-MAC 对应关系。扫描完毕后，选择“数据库”→“保存地址簿”，系统会自动保存对应关系，以备以后使用。



图 10.20　扫描的 IP 地址段选项

10.4.2　查看网关流量

选择“网络性能监视快捷键”→“主机列表”，选中“主机列表”界面左下角的 MAC-IP-IPX 中的 MAC(为什么选择 MAC? 在网络中，所有终端的对外数据，例如使用 QQ、浏览网站、上传、下载等行为，都是各终端与网关在数据链路层中进行的)，如图 10.21 所示。其中数据流量最大的加深部分就是网关。



主机列表：96位置

Hw地址	入埠数据包	出埠数据包	字节	出埠字节	广播	多点传送
0001F4464DC8	0	2	0	294	0	
0001F4603A00	0	1	0	64	0	
000BD4014202	0	6	0	384	6	
000E0C4BA447	0	81	0	5,184	81	
00105CE95AB0	7	0	838	0	0	
00105CE96D21	24	0	3,946	0	0	
00105CEA25BC	334	0	215,704	0	0	
0011091B4885	0	5	0	647	5	
0011091D449E	78,426	0	110,273,179	0	0	
0011091D44C0	345	0	28,594	0	0	
0011091D44F8	0	23	0	2,092	22	
0011091D450B	0	1	0	247	1	
0011091D4A1D	37	0	4,973	0	0	
0011091D4ABF	0	99	0	9,504	99	
0011091D4B1E	2,615	0	1,752,746	0	0	
0011091D4B20	178	0	12,570	0	0	
0011091D4B69	2	0	279	0	0	
0011091DC249	1,438	0	787,771	0	0	
0011093DE403	46	0	5,351	0	0	

MAC　IP　IPX

图 10.21　查看流量

10.4.3　找到网关的 IP 地址

选择“条状图”(本例中网关 IP 为 172.30.37.1)。

172.30.37.1(网关)流量在 TOP 10 图中为最高的，如图 10.22 所示。右边以网卡物理地址方式显示，很容易定位终端所在位置。流量以 3D 柱形图的方式动态显示。本图中 MAC 地址 00110911d449e 与网关流量最大，且与其他终端流量差距悬殊，如果这个时候网

络出现问题，可以重点检查此 MAC 地址是否有大流量相关的操作。

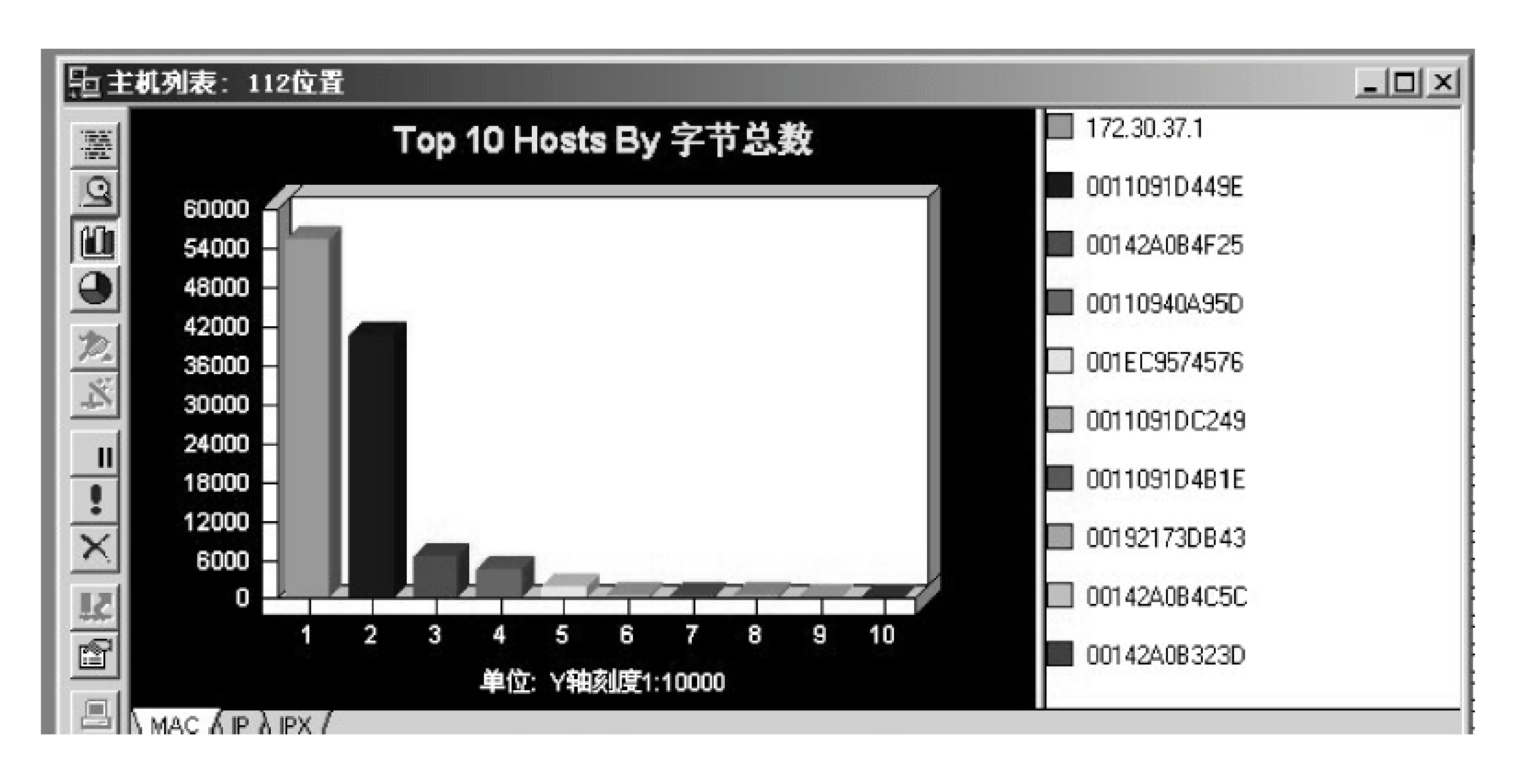


图 10.22　实时流量图

如果要查看 172.30.37.1（网关）与内部所有流量通信图，可以选择"网络性能监视快捷键"，单击"矩阵"按钮，如图 10.23 所示，网关与内网间的所有流量都在这里动态地显示。

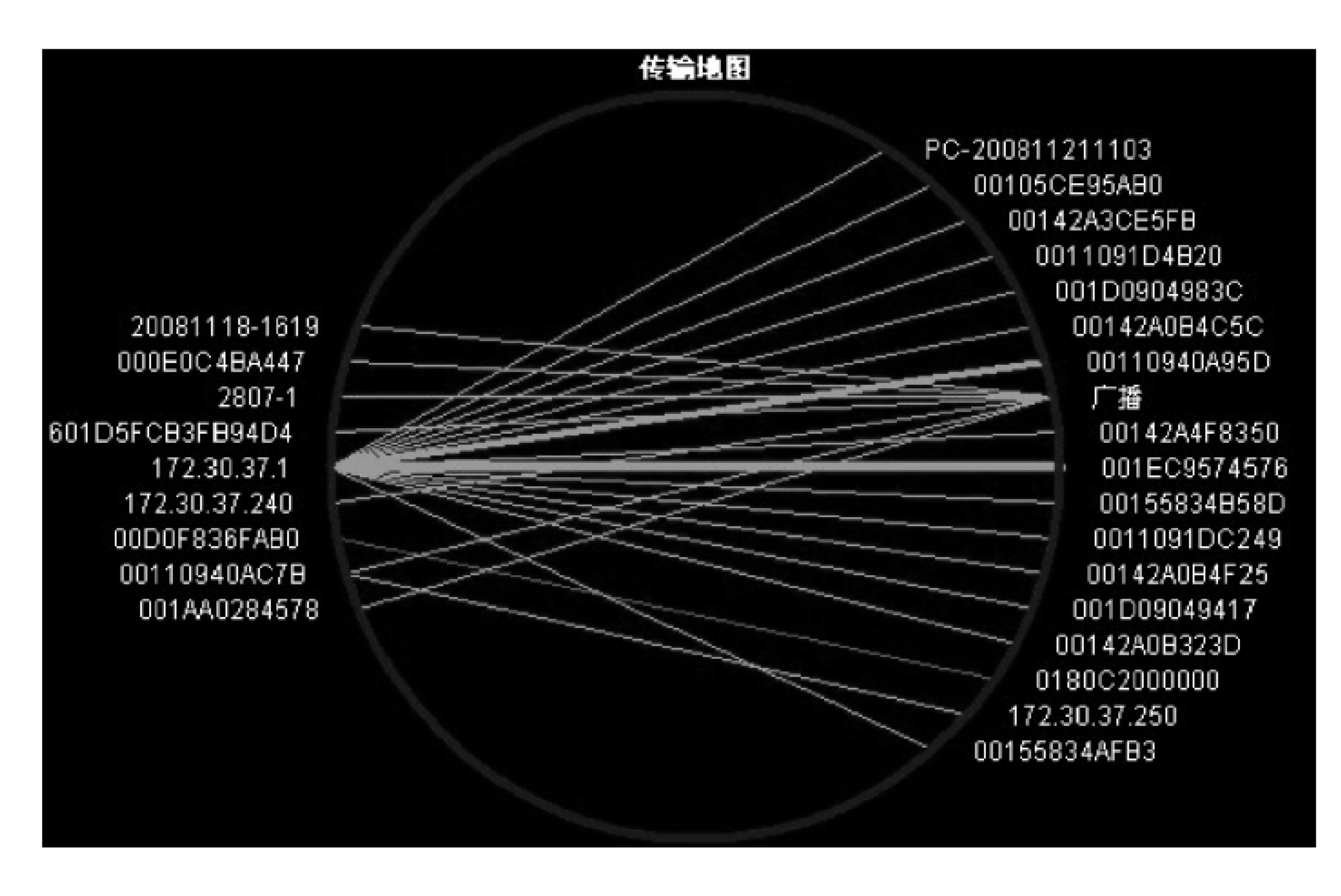


图 10.23　流量通信图

绿色线条状态表示正在通信中；暗绿色线条状态表示通信中断。

线条的粗细与流量的大小成正比。

如果将鼠标移至线条处，程序显示出流量双方位置、通信流量的大小（包括接收、发送）并自动计算流量占当前网络的百分比。

10.4.4　基于 IP 层流量

（1）为了进一步分析 IP 的异常情况，现在切换至基于 IP 层的流量统计图中。选择菜单栏中的"网络性能监视快捷键"→"主机列表"，选中"主机列表"界面左下角的 MAC-IP-IPX 中的 IP。

（2）找到数据量比较大的 IP 地址 172.30.36.84（可以单击数据包排序，以方便查找），选择"主机列表"→"条状图"，如图 10.24 所示。

（3）切换至"矩阵"图形下，看它与所有 IP 的通信流量图，如图 10.25 所示。

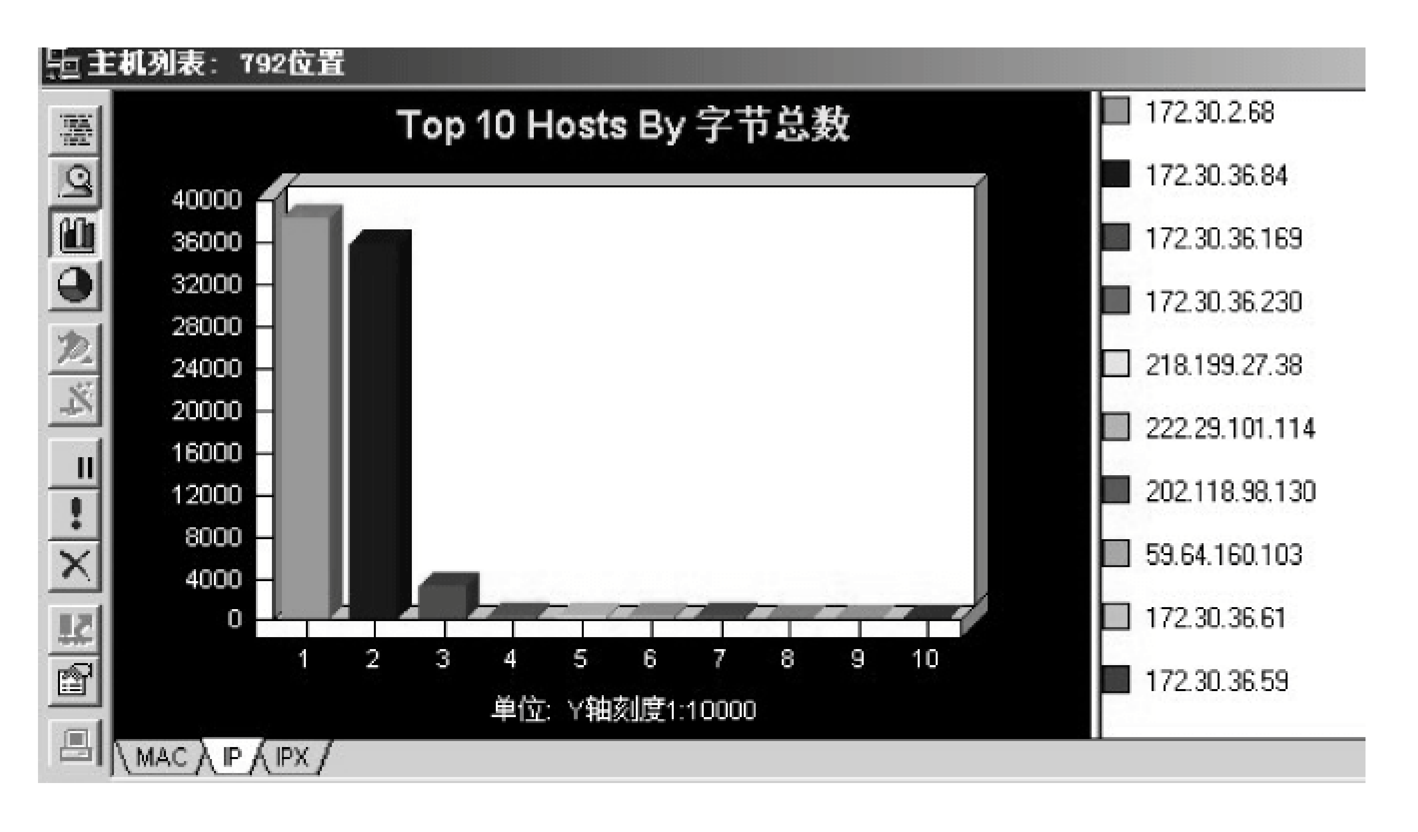


图 10.24　基于 IP 层的流量统计图

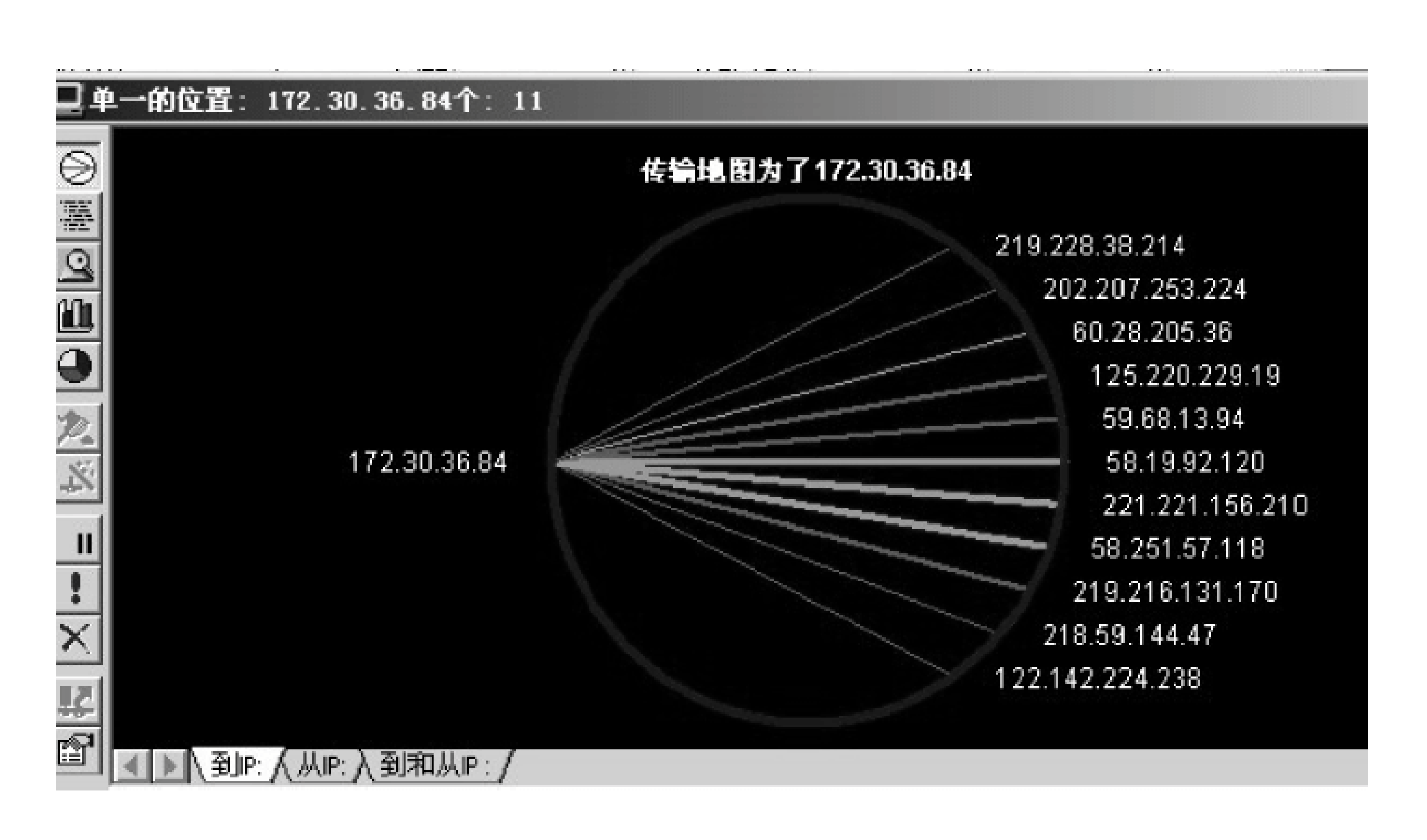


图 10.25　172.30.36.84 与所有 IP 的通信流量图

可以从 172.30.36.68 的通信图中看到与它建立 IP 连接的情况。图 10.24 中 IP 连接数据量非常大，这对于普通应用终端来讲显然不是一种正常的业务连接。可以猜测，该终端可能正在进行观看 P2P 类在线视频的操作。

为了进一步证明猜测，可看 172.30.36.68 的流量协议分布情况。

(4) 如图 10.26 所示，“协议”类型绝大部分为“其他”。在 Sniffer Pro 中，“其他”表示未能识别出来协议，如果提前定义了协议类型，这里将会直接显现出来。

主机列表：1000位置

协议	地址	入埠数据包	入埠字节	出埠数据包	出埠字节
其他	172.30.36.84	359,302	506,596,367	0	0
	172.30.36.169	141,230	128,748,665	0	0
	172.30.36.230	23,155	26,813,924	0	0
HTTP	172.30.36.92	21,888	31,161,022	0	0
其他	172.30.36.59	10,614	1,852,925	0	0
HTTP	172.30.36.61	13,857	15,981,800	0	0
NetBIOS_NS_U	172.30.37.255	5,863	564,702	0	0
其他	172.30.36.208	6,216	512,578	0	0
	172.30.36.117	5,849	587,395	0	0
HTTP	172.30.36.120	5,266	6,464,039	0	0
	172.30.36.59	4,918	2,208,690	0	0
其他	172.30.36.121	4,207	2,758,087	0	0
	172.30.36.85	3,903	909,030	0	0
HTTP	172.30.36.83	3,819	4,252,664	0	0
	172.30.36.121	2,153	1,767,718	0	0
	172.30.36.132	1,952	1,632,877	0	0

MAC IP IPX

图 10.26　Protocol 类型

通过菜单栏中的“工具”→“选项”→“协议”，在第 19 栏中定义 14405(BT 的默认监听端口)，取名为 bt，如图 10.27 所示。



图 10.27　定义监听端口

注意：很多 P2P 类软件并没有固定的使用端口，且端口也可以自定义，因此使用本方法虽然不失为一种检测 P2P 流量的好方法，但并不能完全保证其准确性。具体端口号可根据实际情况进行调整。

10.5　使用 Sniffer Pro 监控“广播风暴”

10.5.1　设置广播过滤器

打开 Sniffer Pro 后，选择“监视器”→“定义过滤器”。首先创建过滤器，并将其名定义为 Broadcast。定义好名称后，选择地址标签下的“已知地址：(Dragable)”选择框，从中展开“主机地址”，将其下的“FFFFFFFFFFFF(广播)”使用鼠标左键拖入位置 1 中或直接输入，如图 10.28 所示。

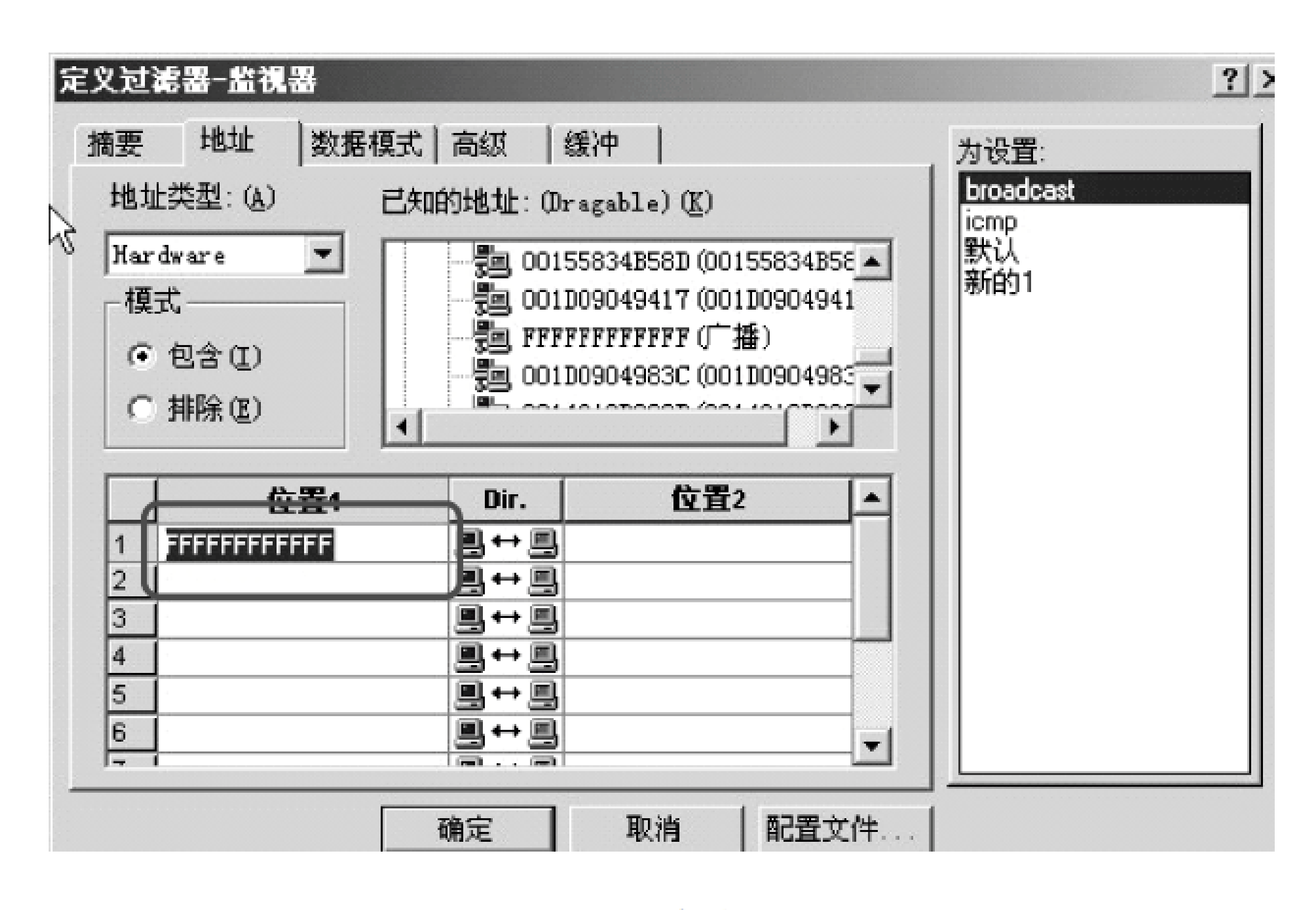


图 10.28　新建广播过滤器

10.5.2 选择广播过滤器

同样在“监视器”菜单下，选择“选择过滤器”，选中刚才定义好的 broadcast，如图 10.29 所示。

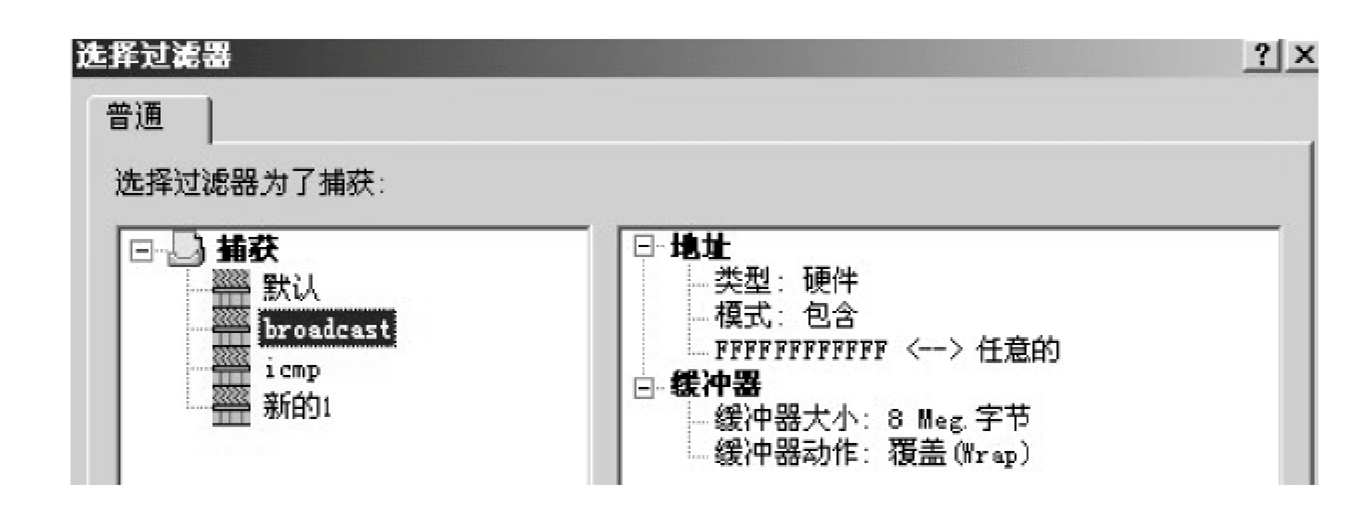


图 10.29 选择广播过滤器

10.5.3 网络正常时的广播数据

先通过 Sniffer Pro 提供的“仪表盘”→“细节”来查看，以下分别是广播包合计统计(如图 10.30 所示)、广播包平均数统计图(如图 10.31 所示)。

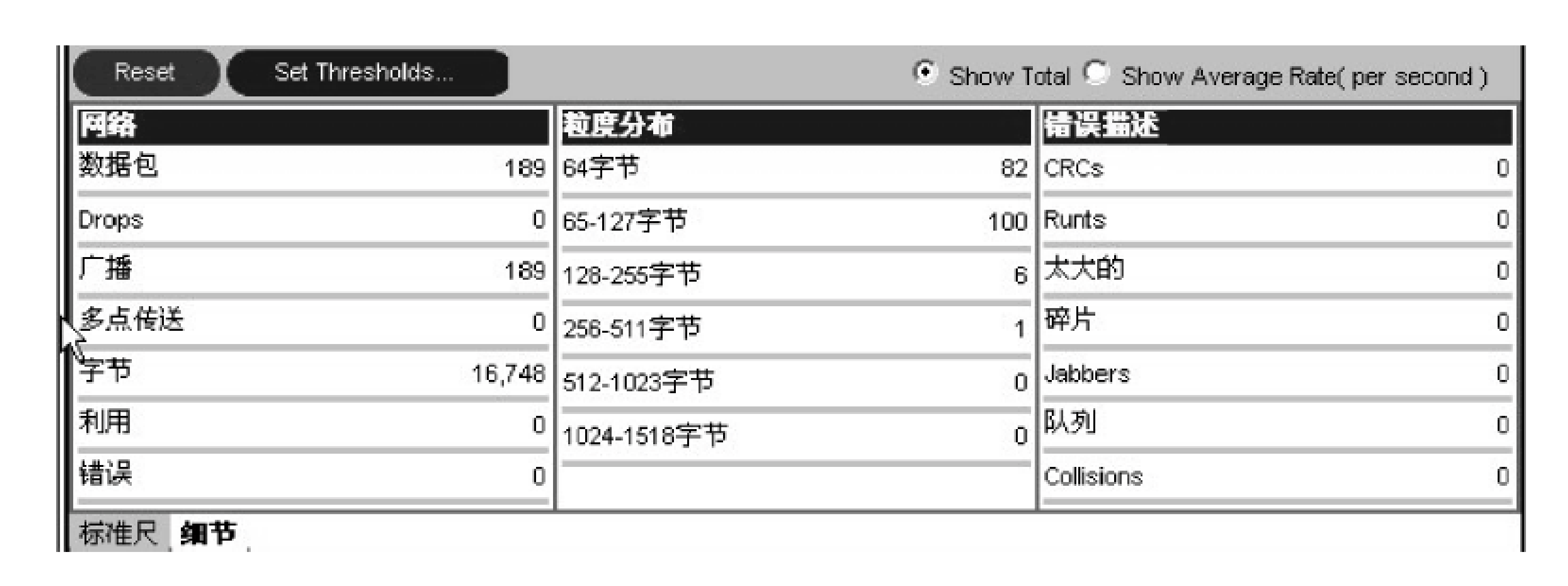


图 10.30 广播包合计统计



图 10.31 广播包平均数统计图

说明：

(1) 由于之前定义好了过滤器，现在所统计的数据均为广播数据。

(2) 在仪表盘详细统计界面，除了统计网络相关数据外，还对数据包大小分布、错误数据包进行详细的分类，以供查看。

(3) 错误数据包捕获和查看，需要专用网卡的支持。

(4) 图 10.30 为截止当前时间，广播数据包合计为 189 个。

(5) 图 10.31 中显示当前每秒平均广播数据包个数为 8 个。

10.5.4 出现广播风暴时，仪表盘变化

下面来看出现如图 10.32 所示拓扑的情况。当虚线的网线连接时就会形成网络环路，在“环路”出现时就会形成“广播风暴”。

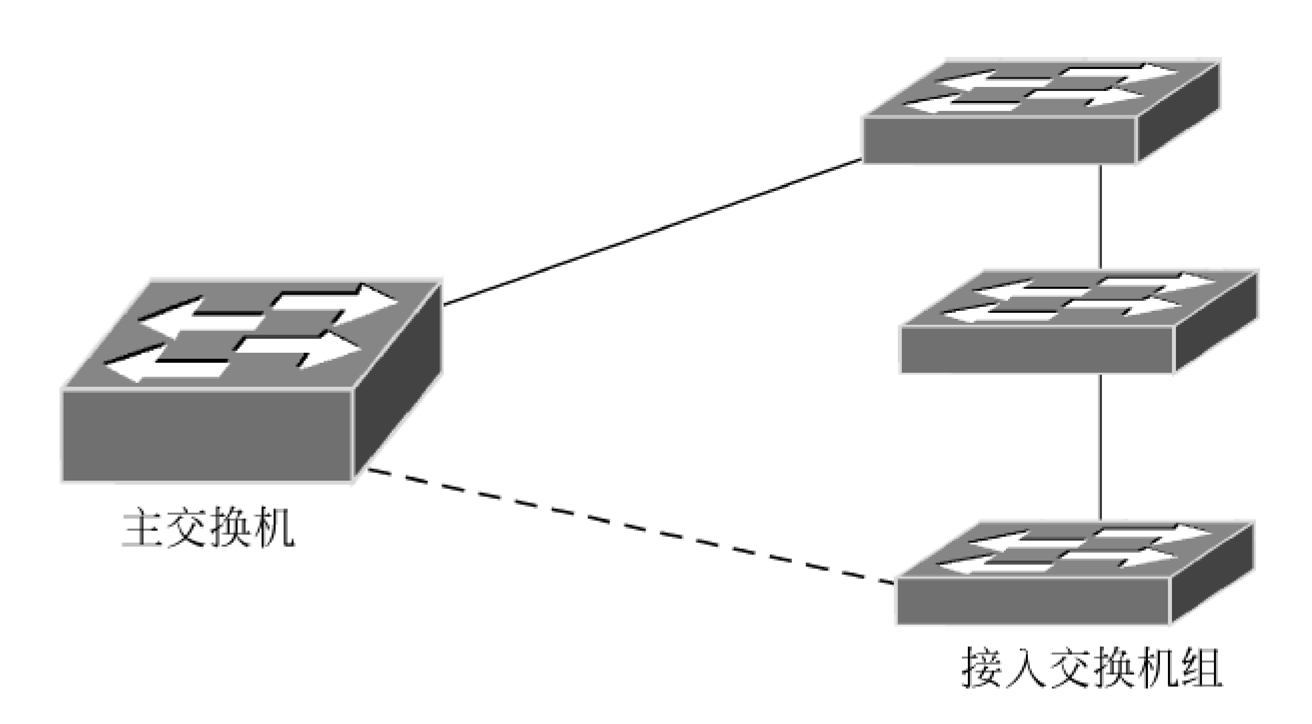
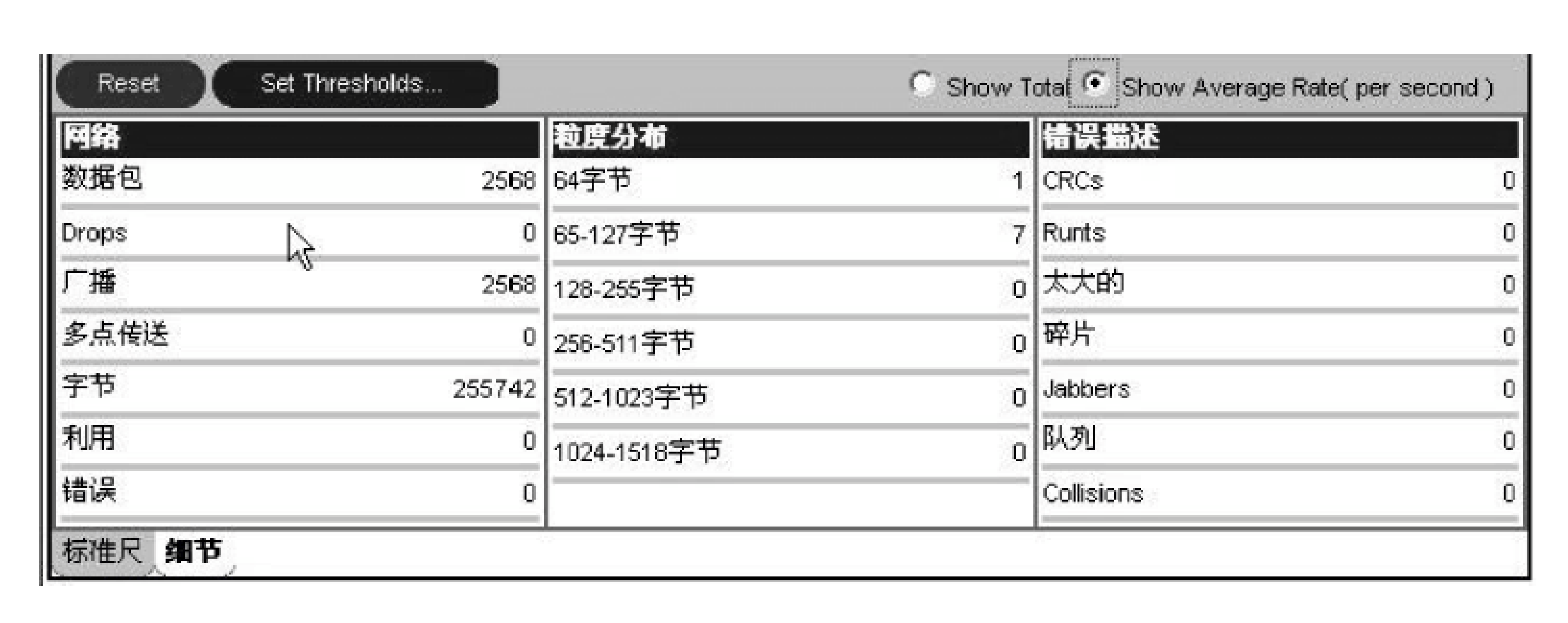


图 10.32 网络环路拓扑图

注意：

如图 10.33 所示，平均广播数据包/秒的统计由刚才的 8 猛增为 2568，广播数据包中的字节数也由 742B/s 增长为 255 742B/S，带宽占用提高了 1000 倍，已经影响了网络的正常运行，应及时查找数据包的来源并排除故障。

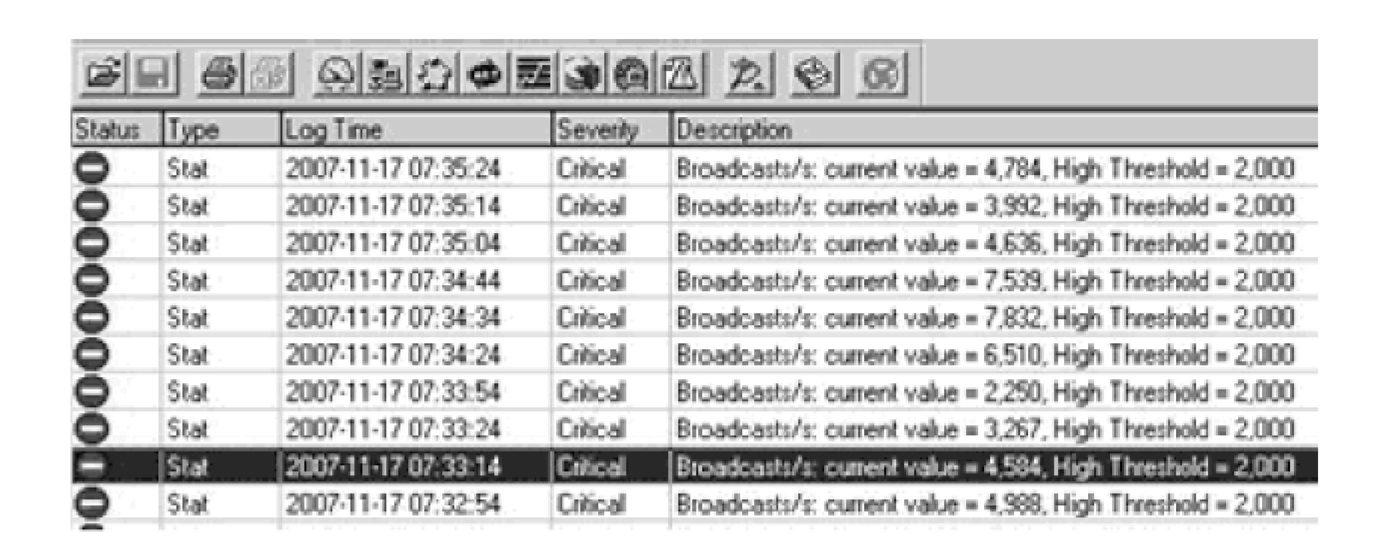


网络		程度分布		错误描述	
数据包	2568	64字节	1	CRCs	0
Drops	0	65-127字节	7	Runts	0
广播	2568	128-255字节	0	太大的	0
多点传送	0	256-511字节	0	碎片	0
字节	255742	512-1023字节	0	Jabbers	0
利用	0	1024-1518字节	0	队列	0
错误	0			Collisions	0

图 10.33 网络流量统计

10.5.5 通过 Sniffer Pro 提供的警告日志系统查看“广播风暴”

如图 10.34 所示，Sniffer Pro 在“广播风暴”时的警告日志。可以通过“监视器”菜单下的“警告日志”查看。软件默认 Broadcasts 为 2000b/s，超过设定的阈值，软件则会报警。



Status	Type	Log Time	Severity	Description
	Stat	2007-11-17 07:35:24	Critical	Broadcasts/s: current value = 4,784, High Threshold = 2,000
	Stat	2007-11-17 07:35:14	Critical	Broadcasts/s: current value = 3,992, High Threshold = 2,000
	Stat	2007-11-17 07:35:04	Critical	Broadcasts/s: current value = 4,636, High Threshold = 2,000
	Stat	2007-11-17 07:34:44	Critical	Broadcasts/s: current value = 7,539, High Threshold = 2,000
	Stat	2007-11-17 07:34:34	Critical	Broadcasts/s: current value = 7,832, High Threshold = 2,000
	Stat	2007-11-17 07:34:24	Critical	Broadcasts/s: current value = 6,510, High Threshold = 2,000
	Stat	2007-11-17 07:33:54	Critical	Broadcasts/s: current value = 2,250, High Threshold = 2,000
	Stat	2007-11-17 07:33:24	Critical	Broadcasts/s: current value = 3,267, High Threshold = 2,000
	Stat	2007-11-17 07:33:14	Critical	Broadcasts/s: current value = 4,584, High Threshold = 2,000
	Stat	2007-11-17 07:32:54	Critical	Broadcasts/s: current value = 4,988, High Threshold = 2,000

图 10.34 警告日志系统

10.5.6 警告日志系统修改

警告日志系统默认阈值都可以修改，选择“工具”→“选项”，然后单击“MAC 阈”选项卡即可，如图 10.35 所示。软件提供了 20 个可以修改的项目，如果觉得利用率在现有网络 50%显得太小，可以将其更改为 80%(快速以太网一般利用率不超过 80%)。而广播 2000b/s 的数值又显得太大，都可以在这里做出更改。

除了可以修改默认阈值外，在系统出现警告时，可以选择通知方式甚至可以使用 Visual Busic 程序自定义动作来打开第三方程序。比如设置告警音，或者通过发送电子邮件等方式通知网络管理员。Sniffer Pro 将警告日志划分为不同级别(严重、重要、次要、警告、通知)，可以在 Alarm 选项卡里做出调整。



图 10.35 修改阈值

10.6 使用 Sniffer Pro 获取 FTP 的账号和密码

使用 Sniffer Pro 程序的数据包分析功能可以方便、迅速地帮助定位 FTP 的账号和密码。由于 FTP 的账号和密码是以明文的形式在网络中传输的，所以可以直接查询到结果。

(1) 选择菜单栏中的“监视器”→“定义过滤器”来定义需要的过滤器。在弹出的“定义过滤器”对话框中选择“配置文件”→“新建”来新建一个过滤器，这里取名为 FTP，如图 10.36 所示。选择“高级”选项卡中 IP 协议下 TCP 协议下面的 FTP 协议作为监控。



图 10.36 新建一个过滤器

(2) 单击捕获面板上的“开始”按钮进行捕获，这时用客户机进行 FTP 的登录，如图 10.37 所示。选择使用用户名为 bob，密码为 123 的用户登录。登录成功后就可以停止捕获。

(3) 打开捕获的数据，在左下角的标签上选择解码，并在显示的数据上面右击，在弹出的下拉菜单中选择“查找帧”，如图 10.38 所示。

(4) 在弹出的对话框中输入 USER，并选择从“摘要文本”搜索，如图 10.39 所示。

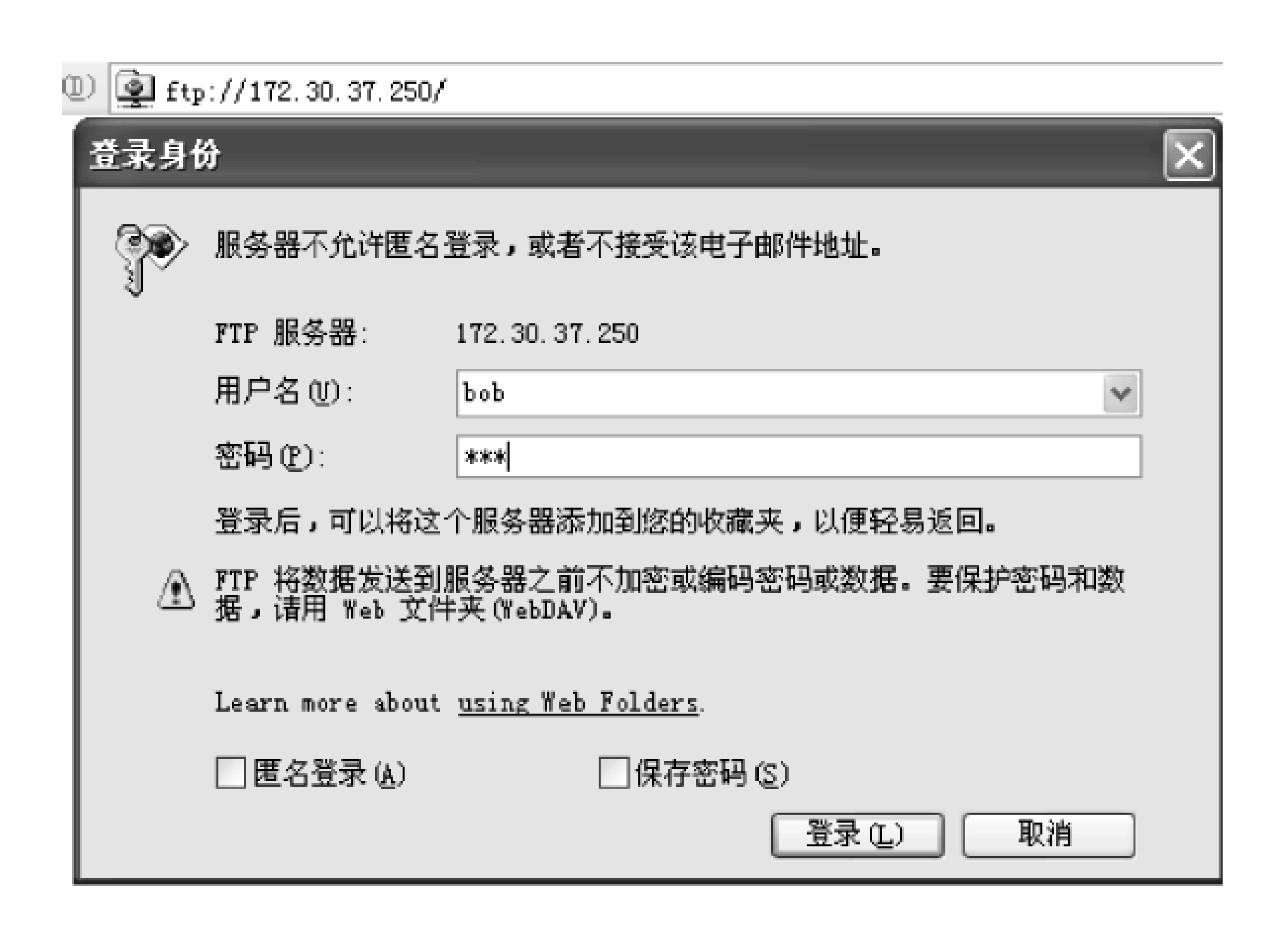


图 10.37　登录 FTP 服务器



图 10.38　查找帧



图 10.39　在对话框中输入 USER

(5) 如果搜索到了匹配的结果，就会看到如图 10.40 所示的 USER bob 和 PASS 123。

通过以上几步可以搜索到网上发布的所有明文的用户名和密码，对于加密的数据虽然能够捕获到，但会显示成乱码，所以有效地保护了数据的安全性。

在网络出现故障时，有经验的网络管理员通常都能够迅速发现故障并加以排除。但在网络日益发展的今天，网络应用、规模、手段都在急速膨胀，仅仅依靠对环境的了解和经验显然是不够的。因此，使用 Sniffer Pro 程序来处理各类网络问题，不失为一种快速有效的手段。

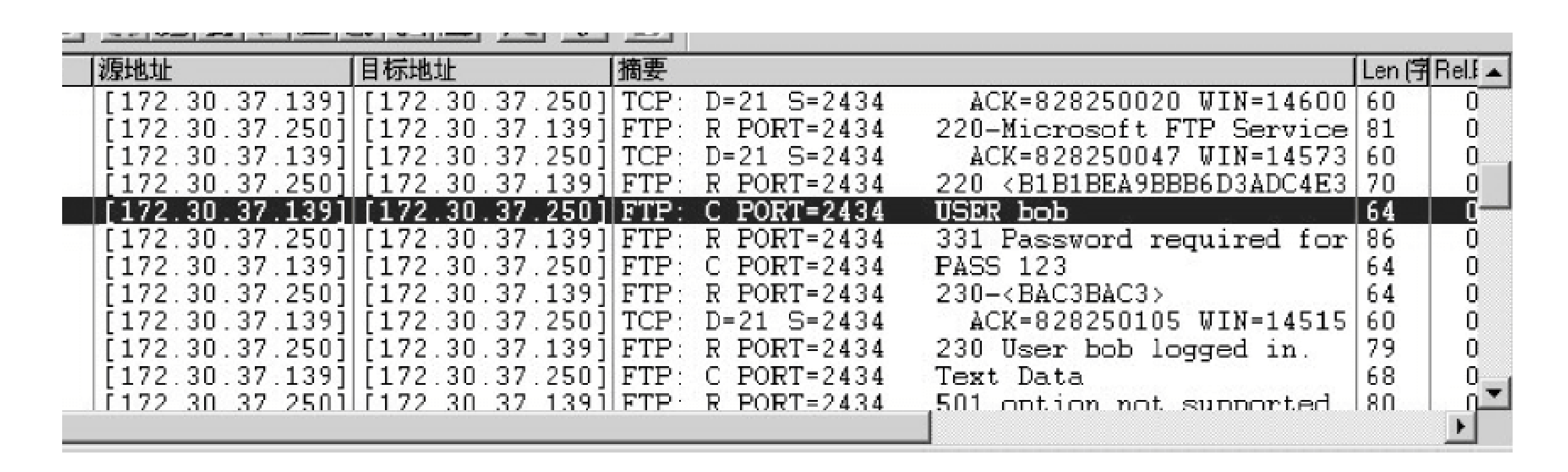


图 10.40 FTP 的用户名和密码

实验思考题

1. Sniffer Pro 对于网络管理员在日常网络维护上有什么好处?
2. 选择什么样的安装位置有助于 Sniffer Pro 获得更加有用的数据?
3. 对于加密数据 Sniffer Pro 还有没有作用?
4. Sniffer Pro 能监控的协议中,数据量比较大的是哪些?

第11章 实验2 网络岗软件的应用

11.1 实验目的及要求

11.1.1 实验目的

通过实验操作掌握网路岗软件的安装与基本功能使用、对于监控软件的原理具有一定的了解。能够实现常用的监控功能。

11.1.2 实验要求

根据本教材中介绍的网路岗软件的功能和步骤来完成实验,在掌握基本功能的基础上,实现日常监控应用,给出实验操作报告。

11.1.3 实验设备及软件

2台安装 Windows 2000/XP 操作系统的计算机,磁盘格式配置为 NTFS,局域网环境、ftp 服务器、准备网路岗软件。

11.1.4 实验拓扑

实验用的拓扑结构如图11.1所示。

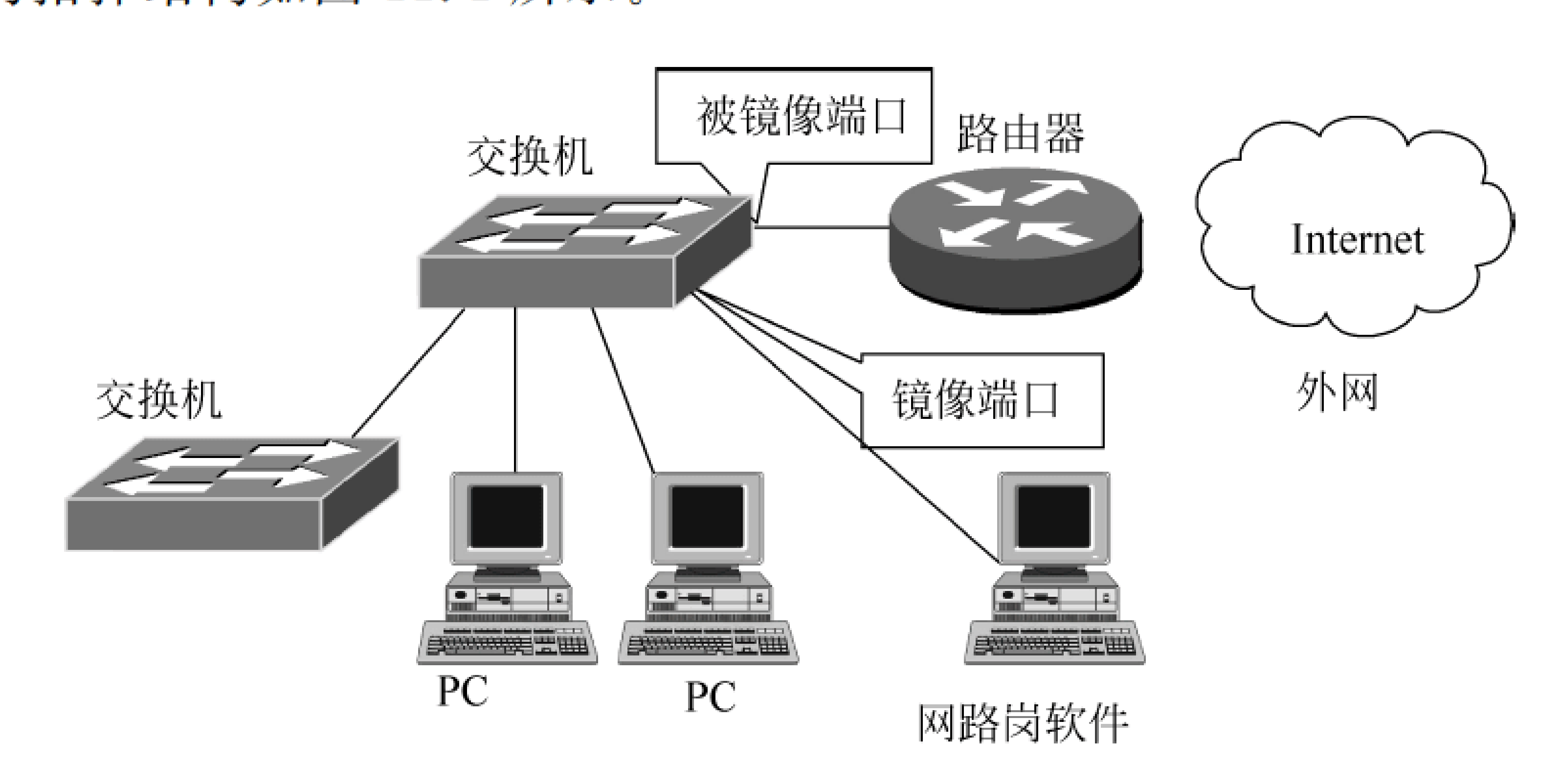


图11.1 实验拓扑

11.2 软件的安装

11.2.1 系统要求

操作系统：Windows XP/2000/2003。

CPU：Pentium 4 或 赛扬 2.0GHz 以上。

硬盘空间：建议硬盘空闲空间不低于 10GB。

监控机器越多，网络流量越大，需要的配置越高，根据以往的经验，P4 以上配置的 PC 上运行网路岗，监控的在线机器可达 500 台以上。

打开安装光盘，请运行安装主监控程序 Sentry5Corp.exe（企业）或 Sentry5School.exe（学校），主程序安装完毕后，如果是第一次在本机上安装“网路岗”产品，则还需要安装光盘中网路岗驱动程序 SentryDrv.exe。

11.2.2 重要子目录

下面介绍安装目录下几个重要子目录：

ETC\子目录存放与系统有关的所有配置文件，如 PcInfo.map 是“基于网卡”网络监控模式的用户信息，UserInfo.map 是“基于账户”网络监控模式的用户信息，IpInfo.map 是“基于 IP”网络监控模式的用户信息。ShareArea.map 存放的是系统配置数据。

如果用户想备份系统配置，只需要备份 ETC 所有文件即可。

CapLog\是系统默认的用来存放监控日志的目录（该日志存放目录可由用户自定义）。

CapLog\Activities\存放的是网络活动日志。

CapLog\WebFiles\存放的是外发资料日志。

11.2.3 绑定网卡

所谓绑定网卡，也就是选择从哪块网卡抓通信包。如果安装本产品的计算机有多块网卡，则用户选择时须小心，一旦选错网卡，“网路岗”不但监视不了任何信息，同时也不能对目标机器进行任何控制。选择网卡如图 11.2 所示。

选择网卡时，用户应选择内网段的网卡，而不能选择接入 Internet 的网卡。出现多块内网网卡时，可能需要用户逐块选择并在“现场观察”窗口测试监控效果。



图 11.2 网卡选择界面

默认情况下，系统获取通信数据包的网卡和发送封堵包的网卡是同一块，但用户可以通过设置信息过滤网卡，以便系统通过另外一块网卡来发送封堵包以控制目标机器。

有一种情况，用户必须启用信息过滤专用网卡。当用户设置“镜像端口”来实现对数据包监视后，但发现不能和局域网其他机器进行通信（假定该机器 IP/网关配置正确），也就是说，所设置的“镜像端口”只能接受通信包，而不能发送数据包，“镜像端口”是单向的。针对这类情况，建议用户再添一块网卡，作为“网路岗”的信息过滤专用网卡。

“信息过滤网卡”在图11.3“高级设置”中配置，配置时，用户必须注意：信息过滤网卡、镜像端口和被镜像端口必须在同一交换机的同一VLAN中。

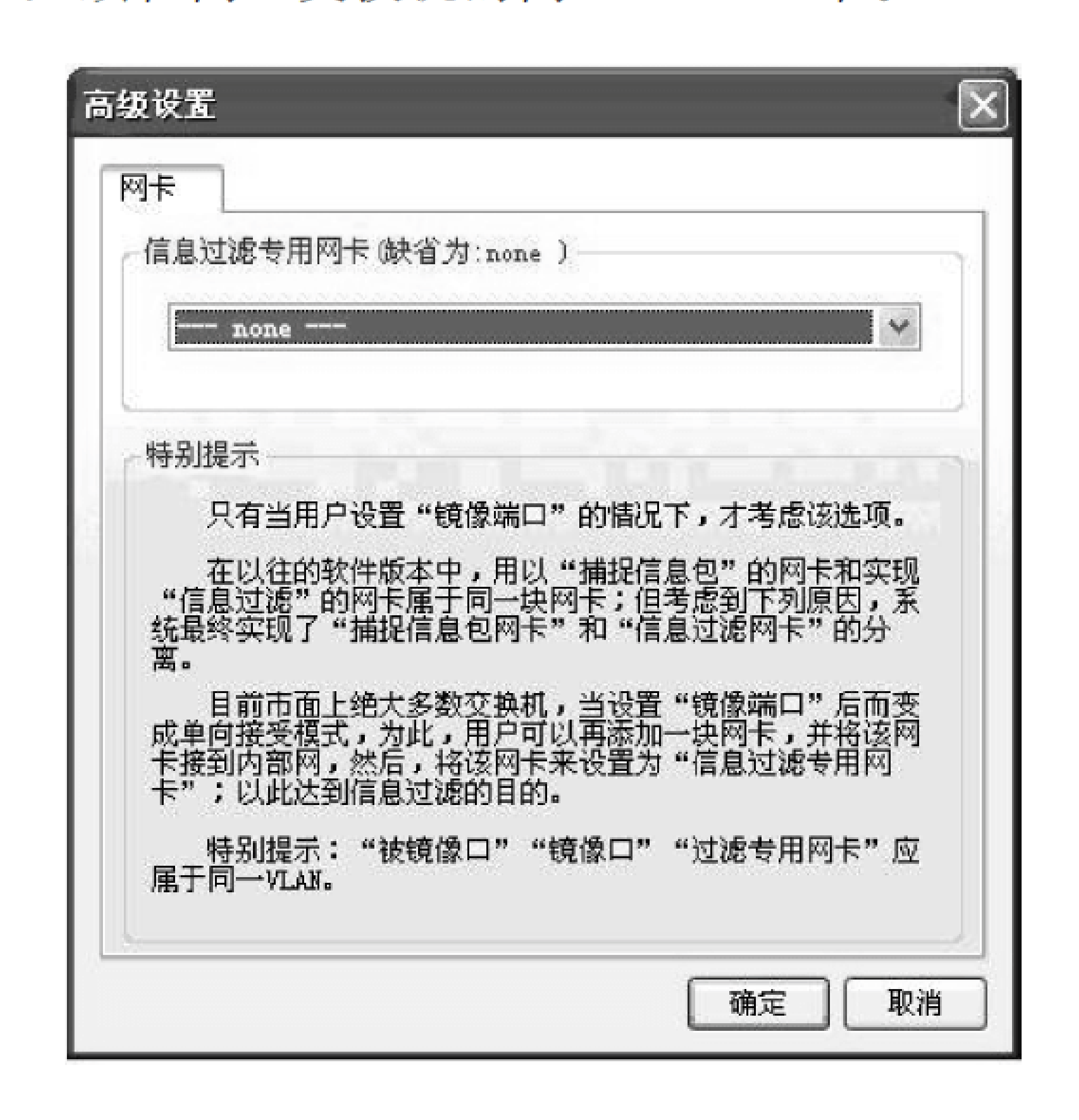


图11.3　信息过滤网卡设置

11.3　选择网络监控模式

网路岗提供了多种网络监控模式：基于网卡/基于账户/基于IP，一般建议监控点在500台以下的情况，选择基于网卡的网络监控模式。用户测试监控效果时，请不要急于对被监控机器进行封堵，建议打开“现场观察”窗口，先观察能否实时监控到目标机器上网站页面的情况。

11.3.1　启动监控服务

进入“服务”栏目，启动所有的后台监控服务。(双击要启动服务的图标)，如图11.4所示。



图11.4　服务栏目

11.3.2　检查授权状态

如果有“网路岗”并口加密狗，请接到打印机并口(同一并口不能级联多个加密狗)，如果监控机上原来有打印连线，则需要取下连线，等接好加密狗后，再将打印机线接到加密狗上。如果有“网路岗”USB加密狗，请在已经安装软件后再将其接入USB插槽，选择“继续安装”，则USB加密狗驱动程序自动成功安装。

注意：插 USB 加密狗前，请先运行本产品的安装程序，如果先插入 USB 加密狗，再安装网路岗，可能导致无法获取加密狗授权信息。

如果手头上有产品序列号，则也可以通过注册序列号来获得授权。注册界面如图 11.5 所示。

用注册码注册时，请务必不要在多台机器上同时用一个号码注册，如果用户要更换机器注册时，必须在原来的机器上“取消本地注册码”，再在新的机器上注册。最后，打开菜单“帮助”——“产品信息”，检查授权的用户数和授权状态。

11.3.3 检查目标机器的监控状态

选择项目“监控策略”→“基于网卡”，先看看是否有机器信息，如果没有，用“搜索邻居”功能试着搜索。每台机器的前面可能有下面的小图标，用鼠标直接单击小图标，其状态可循环改变，如图 11.6 所示。



图 11.5 注册界面

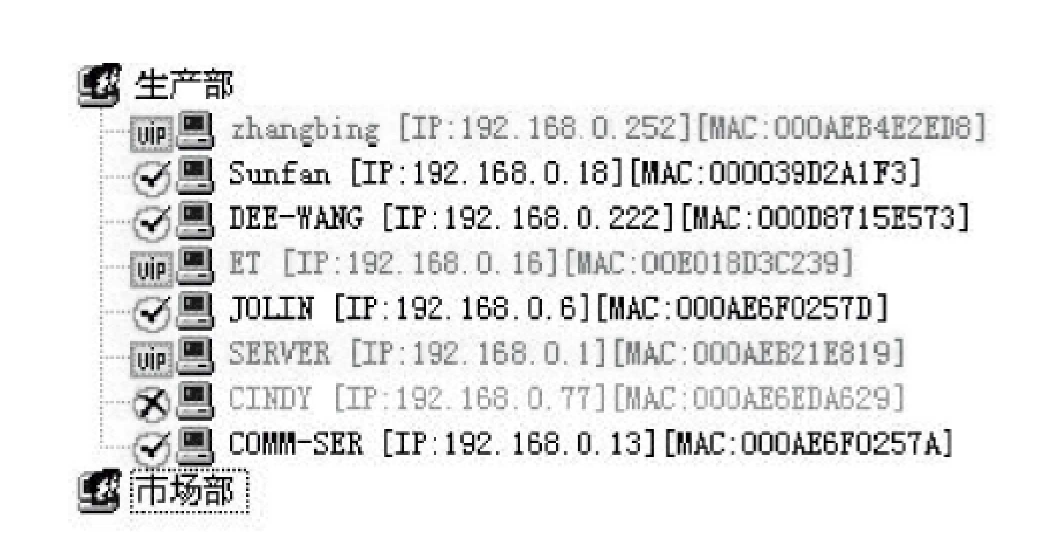


图 11.6 检查目标机器的监控状态

其中 ✓ 表示该机器被监控，VIP 表示该机器不被监控，✗ 表示该机器不被监控但也不允许上网。计算监控点时，以状态 ✓ 为一监控点，超过用户购买的监控点时，系统自动将多余的机器标记为状态 VIP，如果被测试的机器是代理服务器，则应该选其他机器测试。

11.3.4 查被监控的机器上网情况

选择“文件”→“现场观察”，在确保被测试的机器处于 ✓ 状态后，让该机器登录网站，比如 www.baidu.com 等。并留意“现场观察”窗口中是否有对应的信息；如果该窗口中能正确显示目标机器的上网情况，那么说明对该机器的监控是正常的，也说明对该机器的封堵也将起作用。

11.3.5 封锁目标机器上网

选中被测试的机器，进入“封堵端口”子栏目，在 80 端口上打上勾(注：如果用户网络采用代理上网，则上网端口可能不是 80，则需要用户“添加”新的端口，并打勾)，封锁时间段全绿，按下按钮“更新规则=>ET”，最后按“保存设置”使设置生效，如图 11.7 所示。

设置完毕后，再次让被测试的机器上网，并检查“现场观察”窗口下半部分的记录显示。

通过上述几个步骤的测试，可以有效地检测出产品安装是否成功。

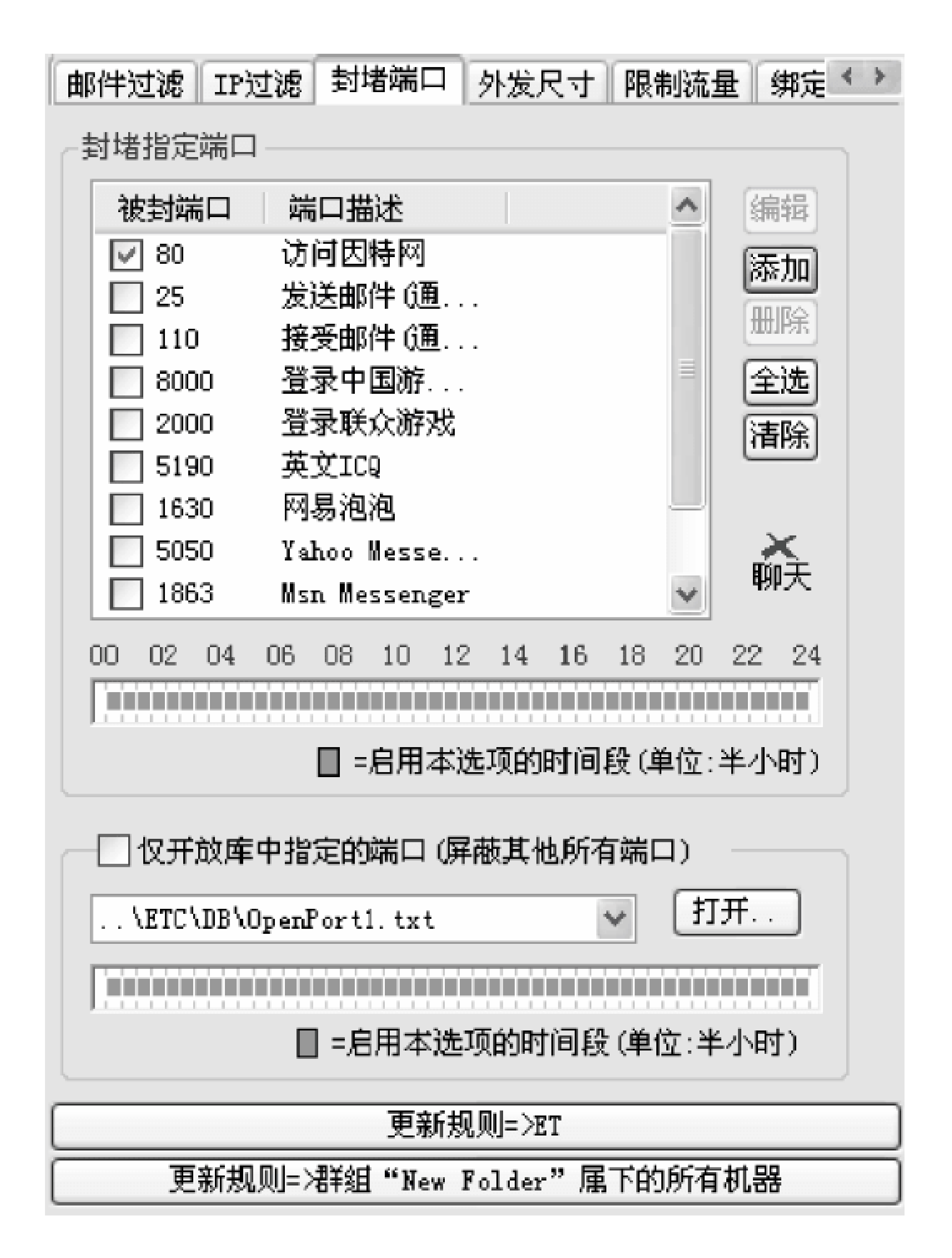


图 11.7　封堵端口

11.4　各种网络监控模式

11.4.1　基于网卡的网络监控模式

1. 基于网卡监控的含义

基于网卡监控就是以网卡 MAC 为依据,根据网卡 MAC 地址确定被监控的信息内容的身份。由于每台机器的网卡 MAC 相对固定,用户不易修改,因此建议将该网络监控模式列为首选。

在这种网络监控模式下,用户更换新的网卡后,“网路岗”会重新检测到新的 MAC,因此,新网卡将被当作新加入的机器来处理,在此提醒用户注意。

2. 基于网卡网络监控模式的实施

(1) 选择网络监控模式,如图 11.8 所示。

(2) 设置监控对象,如图 11.9 所示,包括如下几方面功能:



图 11.8　网络监控模式

“搜索邻居”:自动探测指定 IP 范围内的机器信息(IP 地址/网卡 MAC)。

“新组”:创建新的群组,以便对目标机器进行分组管理。

“转移”:将选中的机器转移到其他部门,用户也可以直接用鼠标将目标机器从一个部门拖到另外一个部门。

图 11.9　设置监控对象

“编辑”：改变某一选中机器的机器名称或改变群组名称。

“删除”：删除选中的一个或多个目标，也可用来删除空的群组。

“查找”：如果目标机器太多，可以用此功能来找出要找的机器。

“解析”：当新机器被加入时，机器名默认为其 IP 地址，如想将 IP 地址转变成机器名，可使用此功能。

“导出”：将目标机器的信息及其对应的规则配置导出到自定义的文件中。

“导入”：将“导出”的机器及规则配置信息从指定的文件加入到当前机器列表中。

“保存设置”：保存用户对“目标机器信息/群组信息/上网规则”等信息的改动。

＜改变目标机器的排序方式＞：单击“搜索邻居”上方的三个 Option 圆按钮，可分别以“机器名/IP 地址/MAC”的排序方式显示目标机器。

＜单选/多选＞单击目标机器，以选择单一目标；按下鼠标左键并拉动，以多选目标，也可用鼠标左键配合 Shift/Ctrl 键进行选择。

＜双击目标机器＞：双击目标机器后，将弹出编辑窗口。

＜更改目标机器监控状态＞：在目标机器的状态小图标上单击，可改变其监控状态。

如果图 11.10 左边部分为空，则需要先启动监控服务，选择绑定正确的网卡，然后，按下“搜索邻居”，输入正确的 IP 范围，开始搜索。

即使不用“搜索邻居”的功能，如果有机器上网，新发现的机器同样可以自动加入；每一目标机器都有相

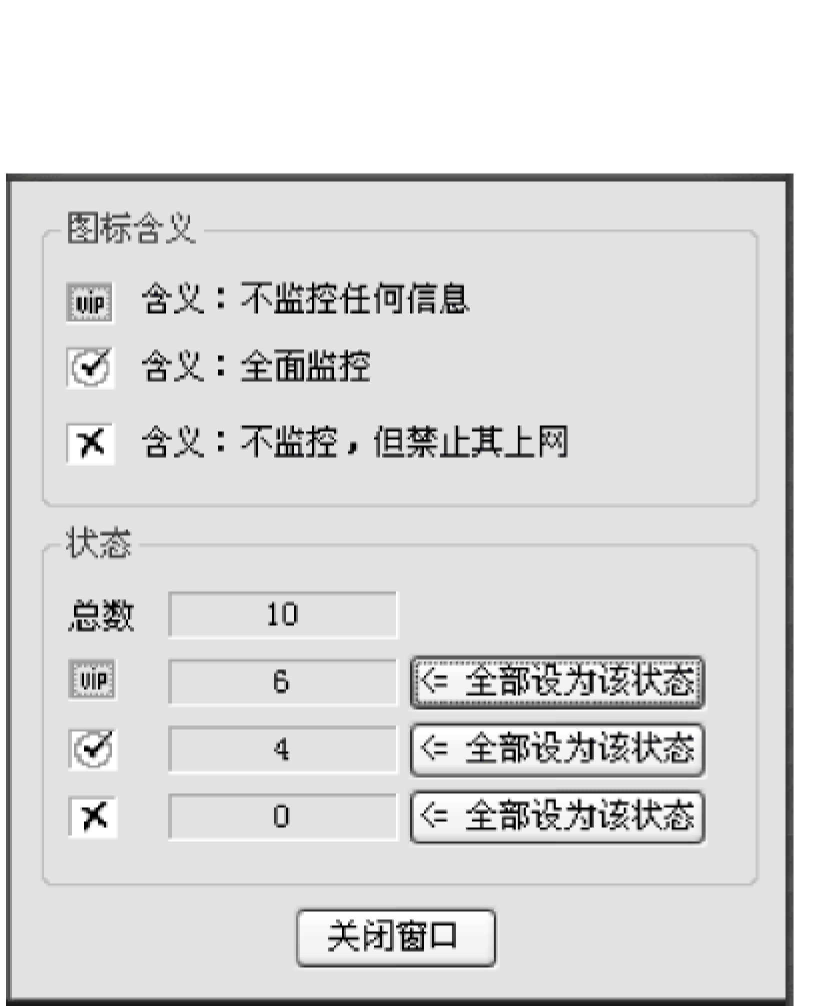


图 11.10　保存设置

应的目录，默认情况下，新机器都放入目录 New Folder 中。

在图 11.10 右边，用户可以设置针对新发现机器的处理方法和默认状态。需要统计所有目标机器的状态，则按下"保存设置"上面的按钮，出现如图 11.10 的画面。

11.4.2　基于 IP 的网络监控模式

1. 基于 IP 监控的含义

基于 IP 监控就是以 IP 地址为依据，并以此 IP 来确定所监控的信息的身份；一个大的网络，比如大学校园网，管理人员通常希望装一套网路岗来解决问题，尽管该网的机器有数千台甚至数万台，且划分的多级 VLAN 多达数十上百个。尽管基于网卡的网络监控模式可以跨 VLAN 监控，但在基于网卡的网络监控模式下，当计算机数量太多，比如超过 1000 台，那么系统会花费较多的资源来探测其他 VLAN 下的目标机器 IP 和 MAC 地址对应情况，最终导致监控效率降低。而基于 IP 监控的方式下，用户可定义一个 IP 范围段来作为一个管理对象。目前，网路岗的客户如果监控点超过 1000，大多采用这种网络监控模式。

2. 基于 IP 网络监控模式的实施：

(1) 选择基于 IP 的网络监控模式，如图 11.11 所示。

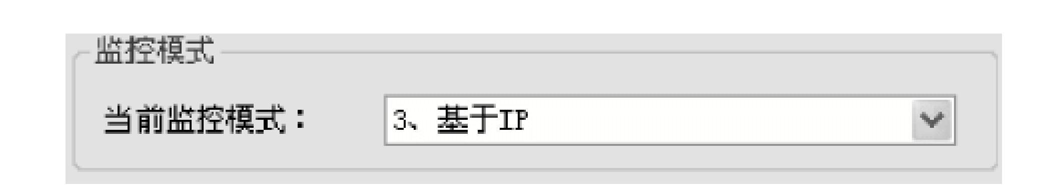


图 11.11　基于 IP 的网络监控模式

(2) 设置监控对象，如图 11.12 所示。

除"手动添加"之外＜监控对象图＞与基于 MAC 地址的网络监控模式基本相同。

"手动添加"：用户手工加入新的 IP 地址或某一 IP 范围；如果用户希望成批加入 IP 地址，则可以先创建范围 IP，然后选中"拆散范围 IP"，如图 11.13 所示。

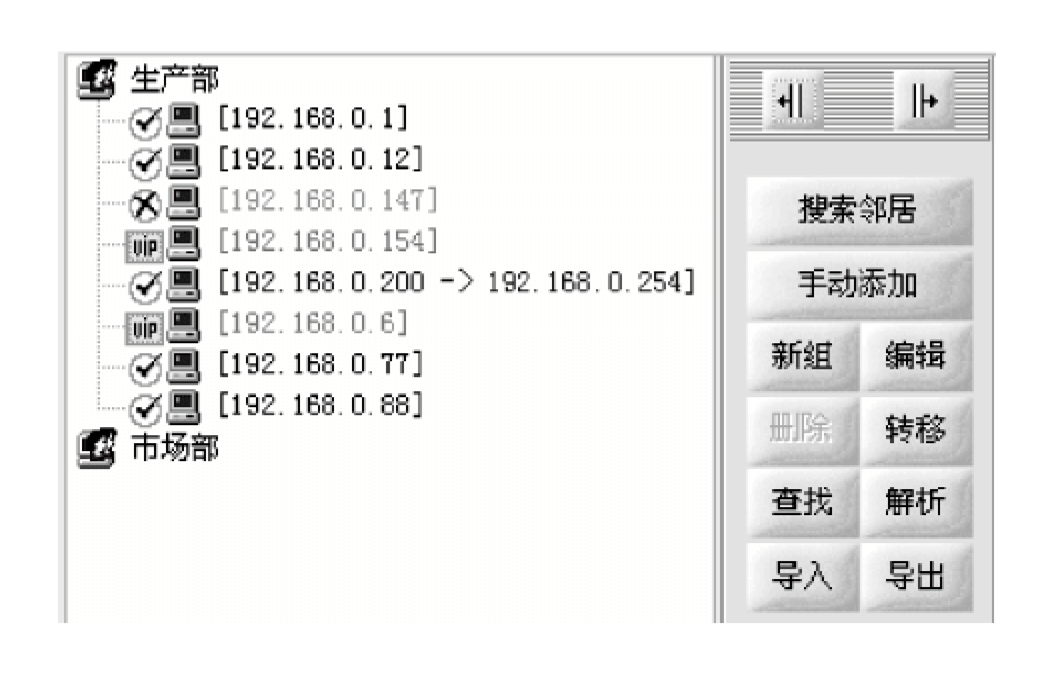


图 11.12　设置监控对象



图 11.13　添加监控对象

11.5　常见系统配置

11.5.1　网络定义

(1) 定义内部网段，如图 11.14 所示。

只有出现多网段/多子网的情况，才需要定义内部网段。定义网段时，一般要求用户定



图 11.14　定义内部网段

义每个需要监控的 IP 段，但是，用户也可采用简化的定义方式，比如：输入 192.168.0.1-192.168.1.255，以简化上图中的输入，这样只需要输入一次。

(2) 设置代理 IP 或内网资源，如图 11.15 所示。

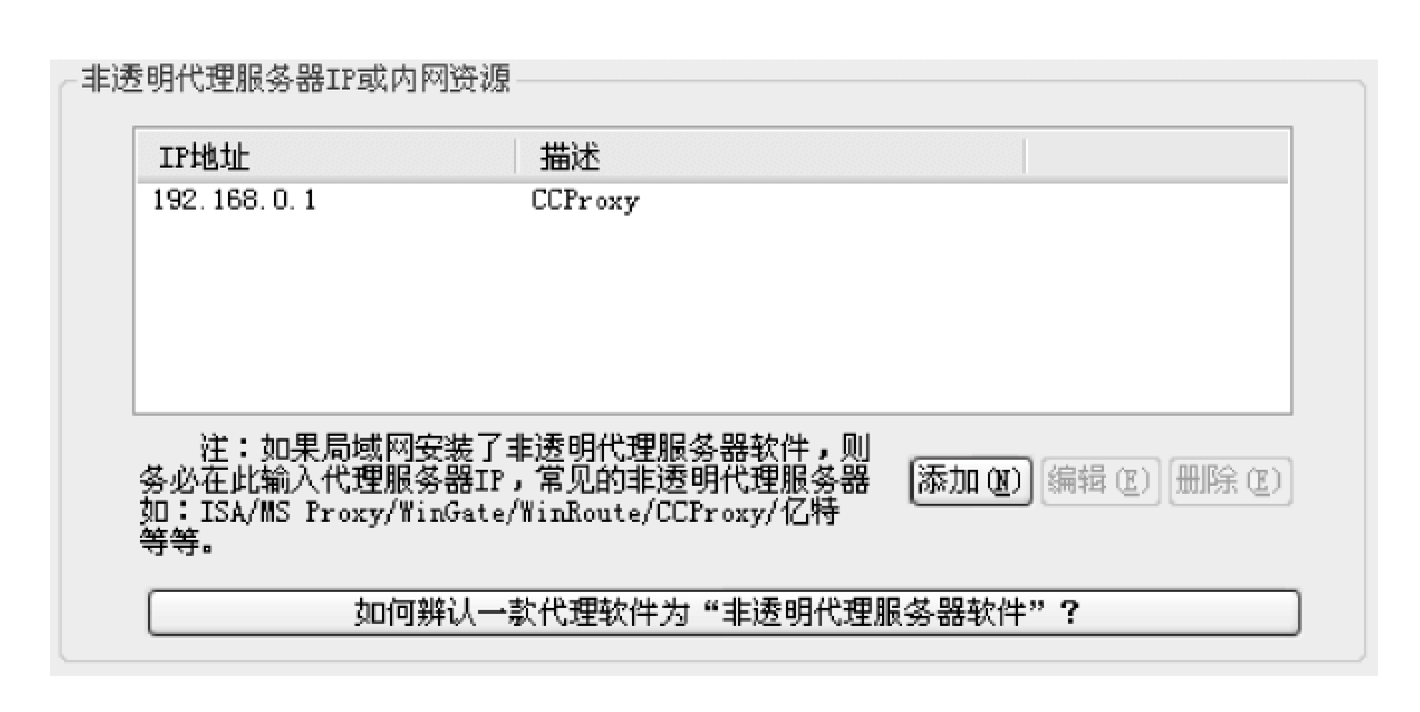


图 11.15　代理 IP 或内网资源的设置

如果用户采用非透明代理服务器软件实现多机共享上网，那么必须在该处输入代理服务器的 IP 地址(内网 IP 范畴)。另外，如果网内有邮件服务器等内网资源，也需要在上面输入其 IP，才能监控到内网机器访问内网资源的情况。

11.5.2　监控项目

默认情况下如图 11.16 所示，所有列出的项目都处于被监控状态，用户可用鼠标单击项目以“取消/选中”该项目。系统还提供了“自定义项目”，用户在定义项目时必须对 IP 通信有所了解，如图 11.17 所示。

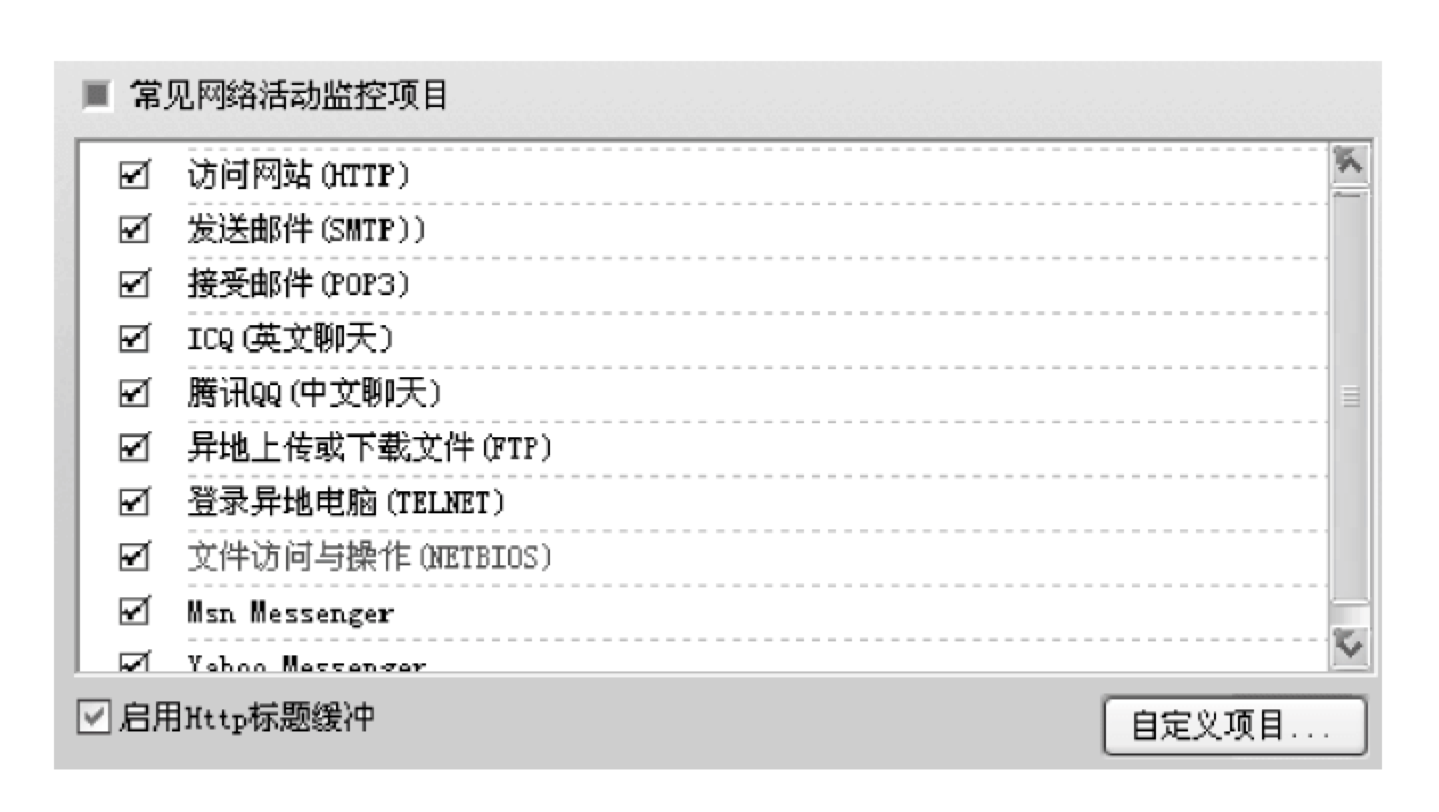


图 11.16　监控项目

图 11.17　自定义项目

“项目名称”用以标识所定义的项目。

“监控描述”将在现场观察窗口中显示并保存于对应的日志文件中。

“通信类型”提供 TCP 和 UDP 两种，以后的版本中将增加其他通信类型。

“源端口”是发出通信包的一方所占用的端口值。

“目标端口”是接受通信方所使用的端口值。

如果系统检测到符合上述条件的通信包，将在现场观察窗口中显示出来，并记录到日志文件中。如果用户了解某个病毒/游戏/聊天软件的通信包规律，端口比较固定，那么通过自定义项目，以让网路岗来提醒用户哪台机器干了什么敏感的事情。

11.5.3　监控时间

该处显示的监控时间是全局的，在非监控时间段，监控服务会完全不做任何控制，尽管服务还处于运行状态。

11.5.4　端口配置

监控项目和端口是息息相关的，系统是通过对特定端口数据的分析来实现对特定项目的监控。每一个项目可同时配置三个端口，比如某网络有一天也许同时有 80、8080、3128 等访问网站的端口的现象出现，这样就需要配置多个端口。

如果用户采用非透明代理服务器软件实现共享上网，且代理端口并非 80，那么就需要 HTTP 的端口 80 后面再增加一个端口值。

11.5.5　空闲 IP

通常，网络管理员在给网内机器分配完 IP 后发现，有些 IP 范围段是空闲的，短期内用不上；同时网管也不想让这些 IP 被使用，那么，利用空闲 IP 防止计算机 IP 被私下更改就非常有效。

11.5.6　深层拦截过滤

如果用户采用的是“非旁路”的监控方式，那么“深层拦截过滤”就会起作用。

(1) 过滤时间安排，如图 11.18 所示，用户可根据需要设置过滤启用时间，该时间是针对所有过滤项目的总体控制。

□星期天 □星期一 □星期二 □星期三 □星期四 □星期五 □星期六

□全天时间(24小时) 从 0 小时 0 分 到 0 小时 0 分

从 0 小时 0 分 到 0 小时 0 分

图 11.18　深层拦截过滤设置

(2) 过滤项目定义，以过滤 UDP 登录方式的 QQ 为例：如图 11.19 所示，这里设置的 Port 8000-8001 是针对每条通信的外网端口的。其他通信端口的过滤设置方式类似。



图 11.19　通信端口的过滤设置

除了上述过滤项目外，由于考虑到对 NAT 性能的影响，系统暂时不提供过多的过滤功能设置。

11.6　上 网 规 则

11.6.1　上网时间

如图 11.20 所示，如果用户只是简单地控制目标机器的上网行为，在这里设置是最好的。图 11.20 中蓝色显示块表示允许，白色表示禁止。用鼠标控制选择蓝色/白色。

只有在白色时间段，对 Web 端口的封堵选项才起作用。在蓝色时间段是不是就一定可以上网还难说，主要看后面的项目中是否设置了封锁，在如此多的上网规则中，只要有一处封堵，就能起到封堵的作用。

如果用 outlook 收发 hotmail 邮件，图 11.20 中的选项将不起作用，因为 hotmail 邮件并非通过收发邮件的端口(110/25)进行通信，而是通过 HTTP 方式。

11.6.2　网页过滤

如图 11.21 所示，网页过滤主要是针对地址 URL 的过滤，对内容不予考虑。定义关键词的时候，建议输入最具代表性的词。针对 google.com、baidu.com 和 3721 等搜索网站，还支持对中文关键词的封堵。



图 11.20　上网时间设置

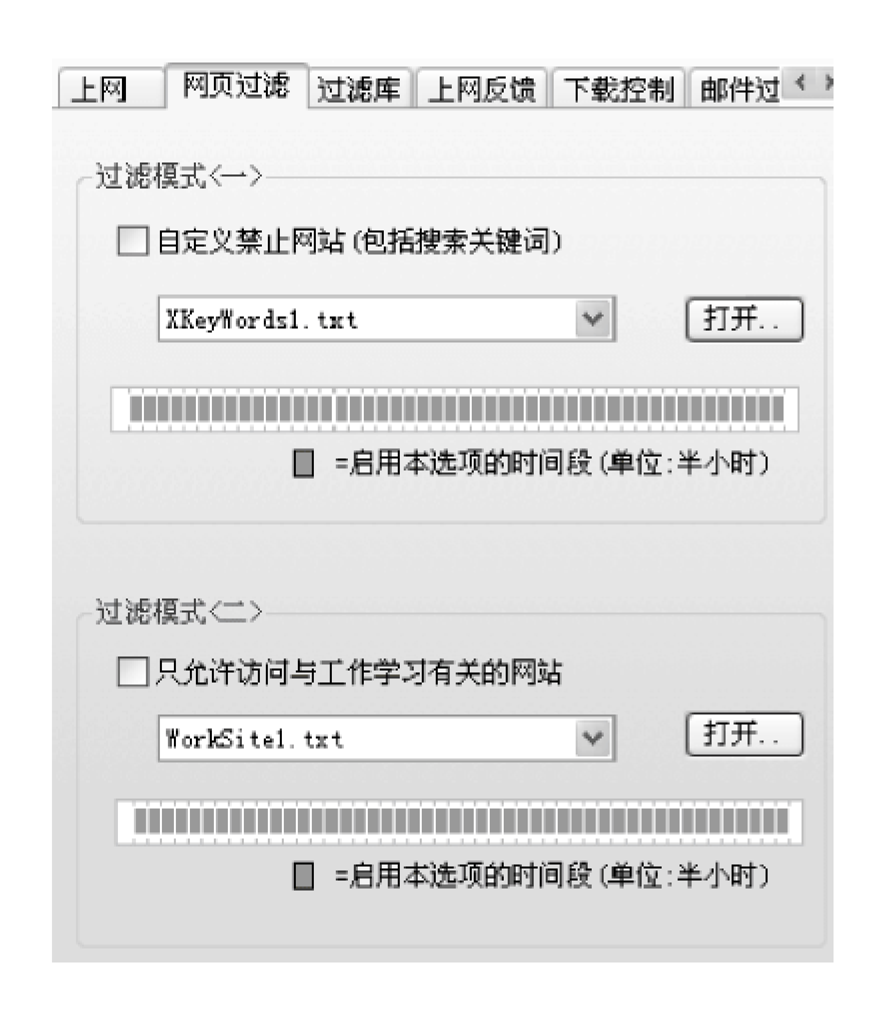


图 11.21　网页过滤

举例说明：

(1) 如果要禁止上 www.sina.com.cn 网站，则输入 sina.com.cn 比较合适，如输入 sina.com 的话，则被控机器连同 www.sina.com 和 www.sina.com.cn 都不能上了。

(2) 在禁止网站列表中输入“法轮功”，以防被控机器在搜索网站上以该关键词来搜索。

(3) 在“只允许访问列表”中输入 sohu 可让用户只能上 www.sohu.com。

11.6.3　过滤库

如图 11.22 所示，为方便用户控制，“网路岗”收集了几类网站列表和端口库，可供选择。针对列表库，用户可进入“列表库管理工具”进行添加或删除操作。

“列表库管理工具”是专门针对网站列表库的工具，用户可以随意添加/删除/查询现有的列表库。如果用户有现成的列表文本文件，则可以导入到相应已打开的库中，那些被成功导入的网站将被显示出来，通过“导入”与“导出”功能，用户之间可以轻松交流自己收集的网址。

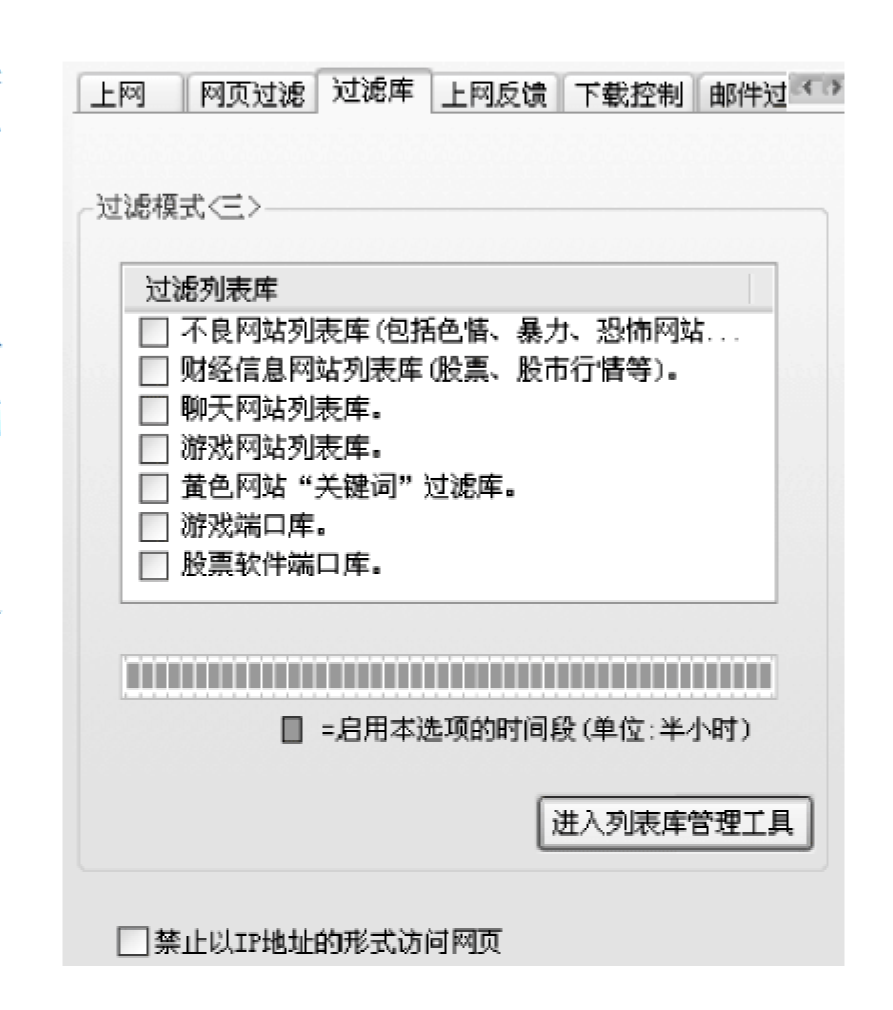


图 11.22　过滤库

11.6.4　上网反馈

如图 11.23 所示，如果用户通过封堵端口的方式来禁止上网，则上述功能无效；必须通过关键词来封锁网站才有效。

如图 11.23 中的默认设置所示，根据用户需求，让被封锁的机器显示更明确的信息。另外如果目标机器上了某个敏感网站，通过设置也可以让其跳转到某一个指定的页面(比如企业网或校园网)。

11.6.5 邮件过滤

如图 11.24 所示，邮件过滤并非严格过滤，这是因为如果邮件内容太少，甚至没有，那么系统检测到用户有邮件发送迹象时，已经太迟，该邮件可能已经发送出去，再去堵截就没有意义了。尽管如此，针对稍大的邮件的过滤还是有效的，尤其是带附件的邮件。



图 11.23 上网反馈设置

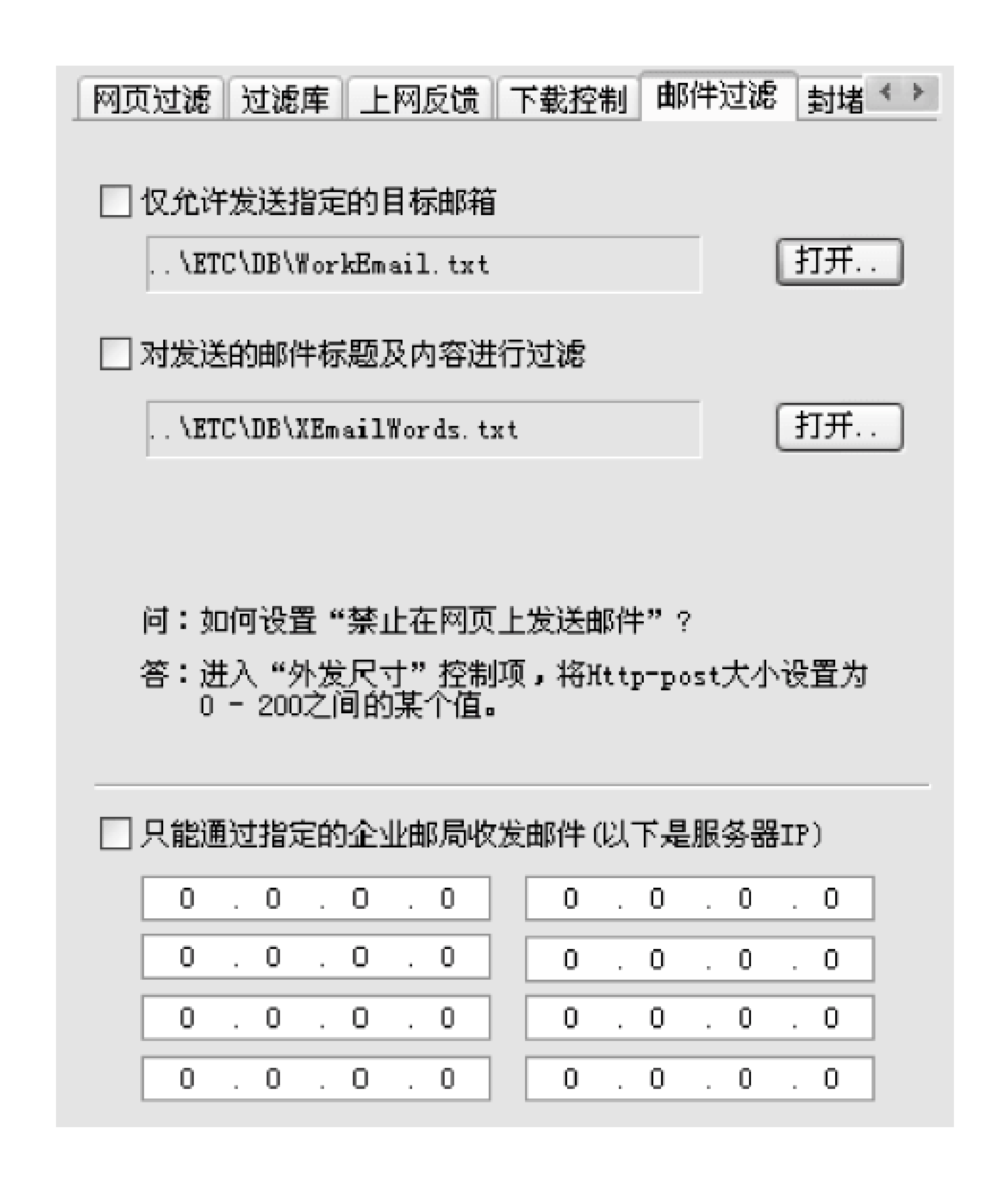


图 11.24 邮件过滤

11.6.6 IP 过滤

如图 11.25 所示，IP 过滤是针对因特网上各类资源的 IP 地址的过滤，进行设置时，需要对 IP 有全面的了解。事实上，全球 IP 地址的分配是有一定规则的，相关知识可在网上搜索到，搜索关键词请用“IP 地址分配”。利用这些规律，可以设置某些地区的网站禁止访问。某些大型网站，比如 yahoo、sina 等都具有很多的 IP 地址，因此，不能简单通过一两个 IP 地址来封锁该网站。



图 11.25 IP 过滤设置

11.6.7 封堵端口

如图 11.26 所示，任何一款网络软件，如果它建立在 TCP/IP 通信之上，都会用到“端口”，比如股票软件、FTP 软件、收发邮件软件等，都具备自己的开放端口。因此，通过“端口”来封锁上网行为是非常有效的。

尽管很多软件的端口是软件开发者自定义的，但用户也不必担心软件改变自身的“开放端口”，因为“开放端口”一旦改变，该软件的客户端也必须随之更改，从市场角度看是不现实

的。如果了解 IP 包的话，用户可利用本系统提供的工具“IP 包分析工具”来分析端口。

11.6.8 外发尺寸

如图 11.27 所示，这里对外发尺寸的控制是一种模糊控制，并不能精确到字节数，而且，上述功能只有在用户购买的版本具备邮件内容的监控功能时才起作用。原因是，没有内容监控的话，系统无法及时知道外发文件的大小，也就不能在中途进行堵截。

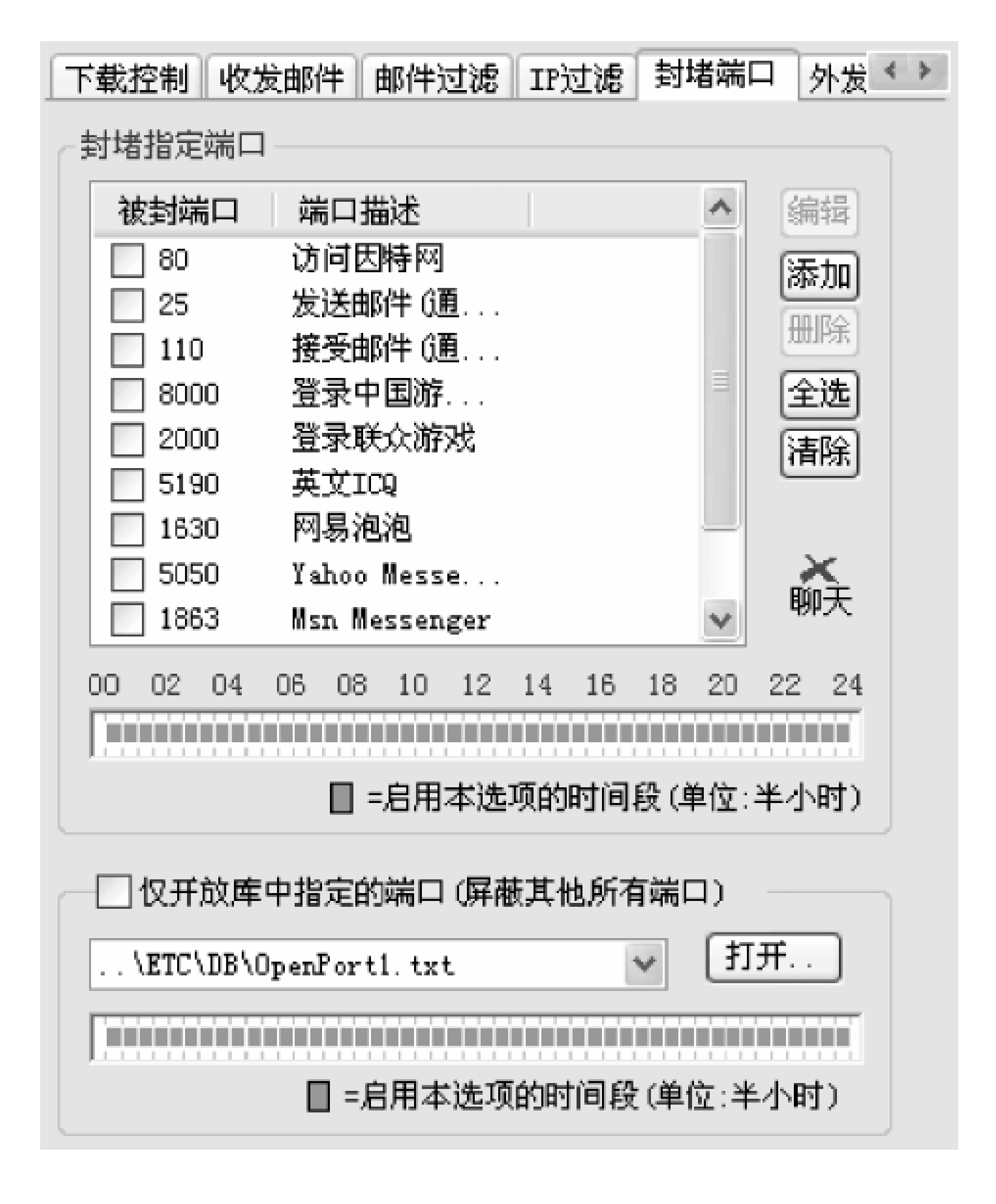


图 11.26 封堵端口设置

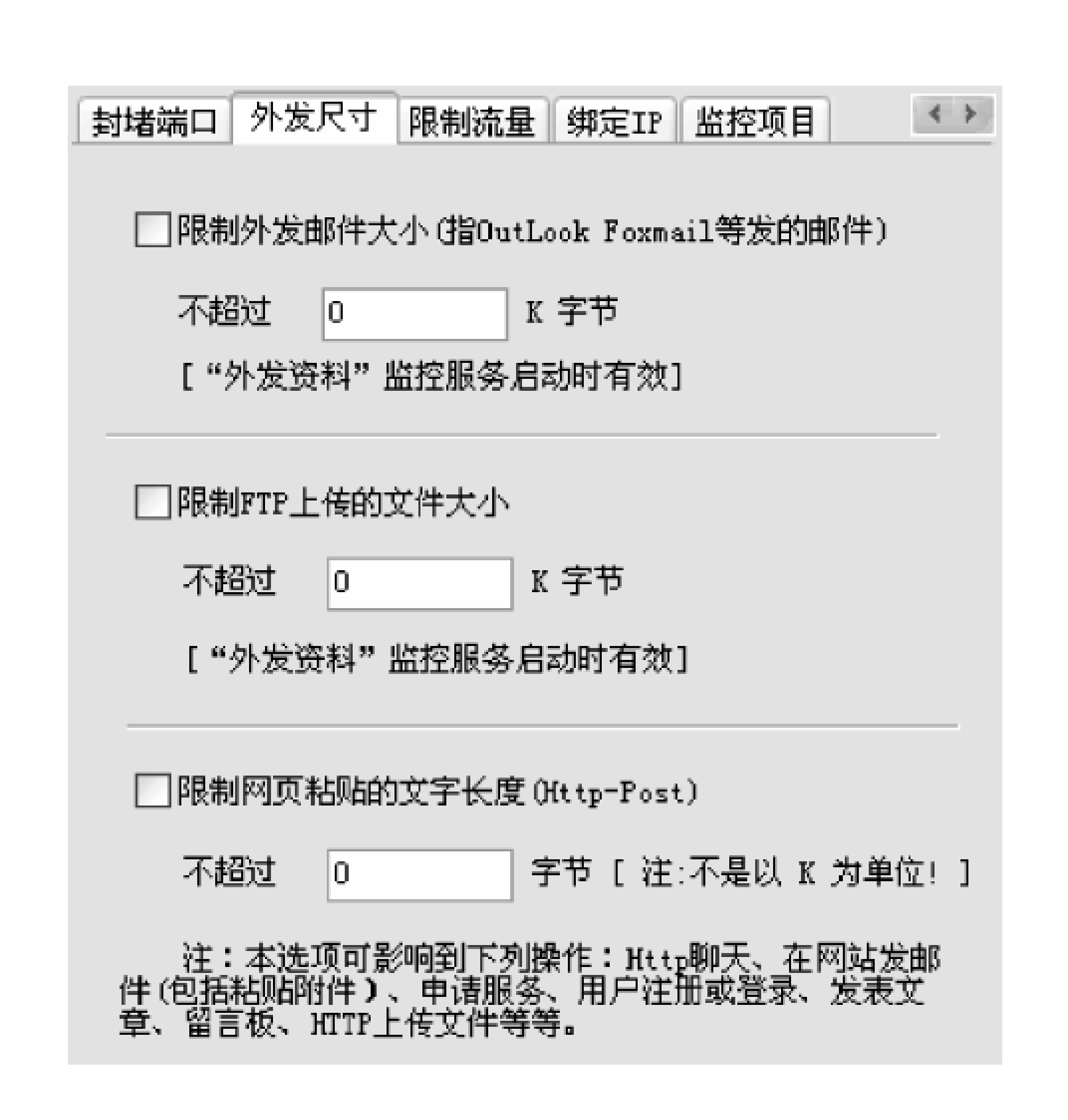


图 11.27 外发尺寸设置

11.6.9 限制流量

如图 11.28 所示，本软件只能检测到上网带宽数据而不能实现对带宽的管理和分配。根据需求，提供了对流量的限制功能；比如，限制某台机器每天只能有多少 M 的上网流量，超过这个数字，系统会自动断网。

图 11.28 显示的累计流量是动态的，便于用户及时观察到客户机的流量。如用户规定该机器每分钟的流量，则每隔一分钟累计流量就会自动变成 0。

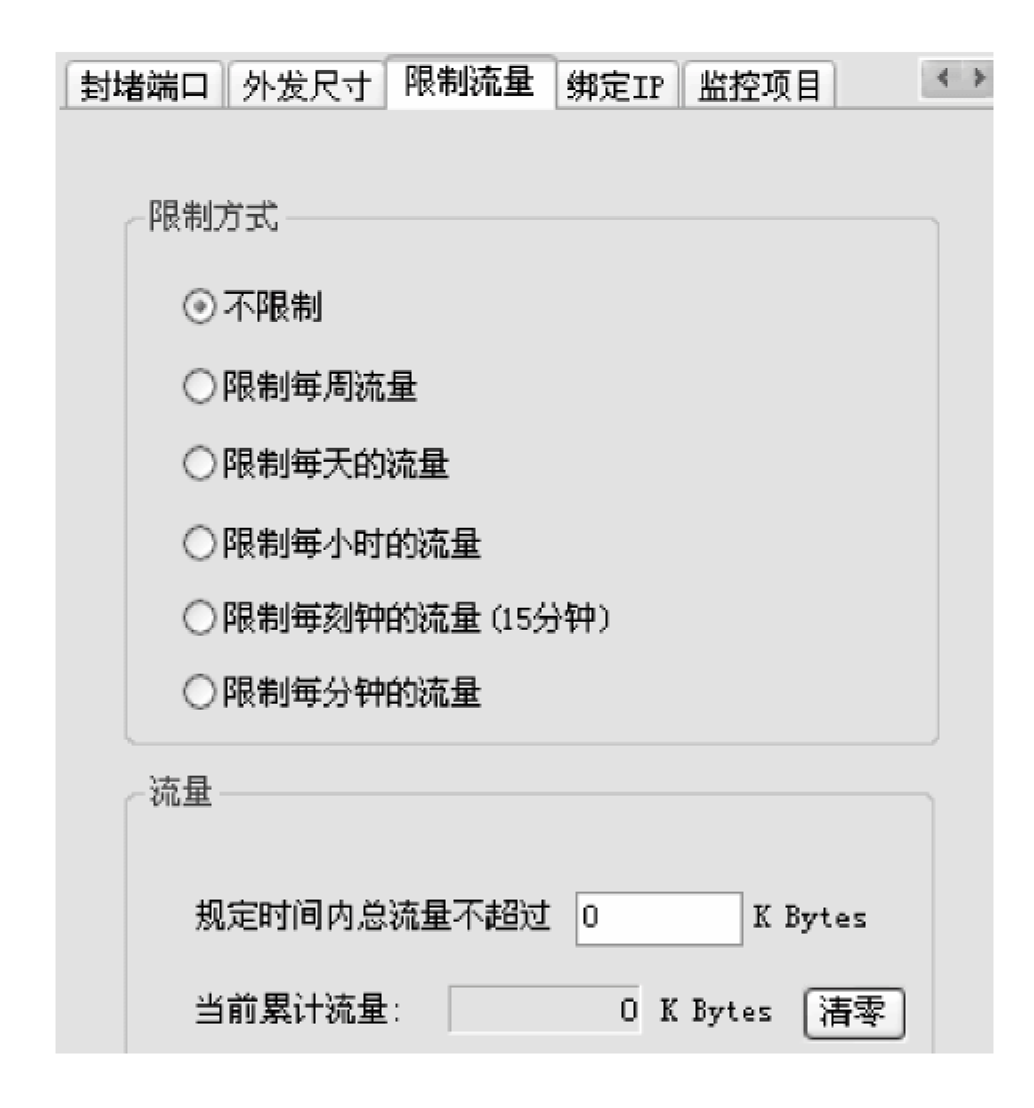


图 11.28 限制流量设置

11.6.10 绑定 IP

如图 11.29 所示，在单网段环境，且是基于网卡的网络监控模式下，用户可以通过绑定 IP 的功能来防止目标机器私下更改 IP 上网。选项：“IP 改变时，记录其变化情况”被选中时，该网卡更改 IP 地址后，会详细记录其更改情况。

11.6.11 监控项目

如图 11.30 所示，用户可根据需要设置目标的监控内容。如果用户购买的版本没有邮件内容监控或没有聊天内容监控，则图 11.30 中“监控聊天内容”和“监控外发资料内容”的选项就不起作用。如果用户只是想过滤邮件正文而不记录邮件的话，则可以选择“只过滤发送邮件的内容，不生成邮件日志”。

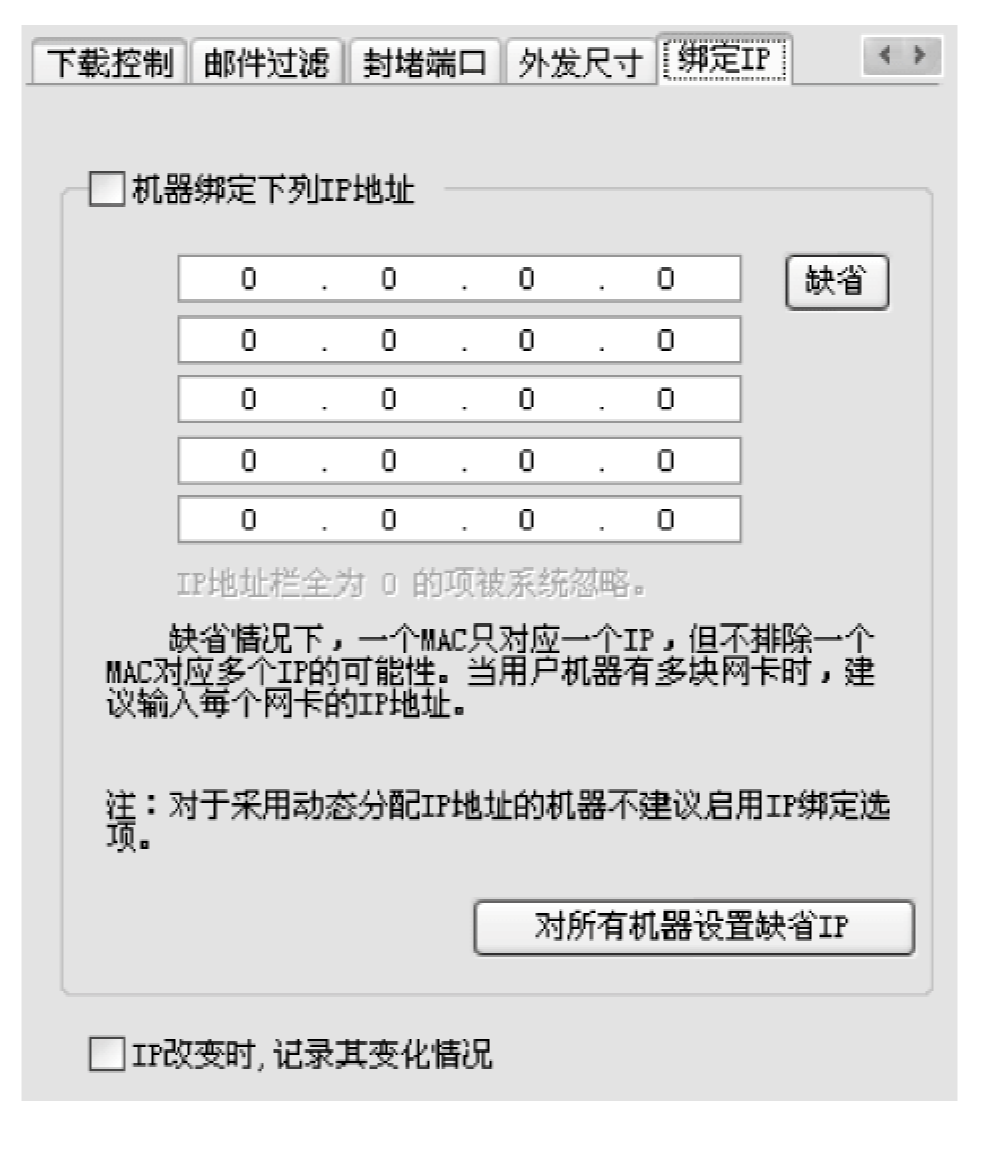


图 11.29　绑定 IP 设置

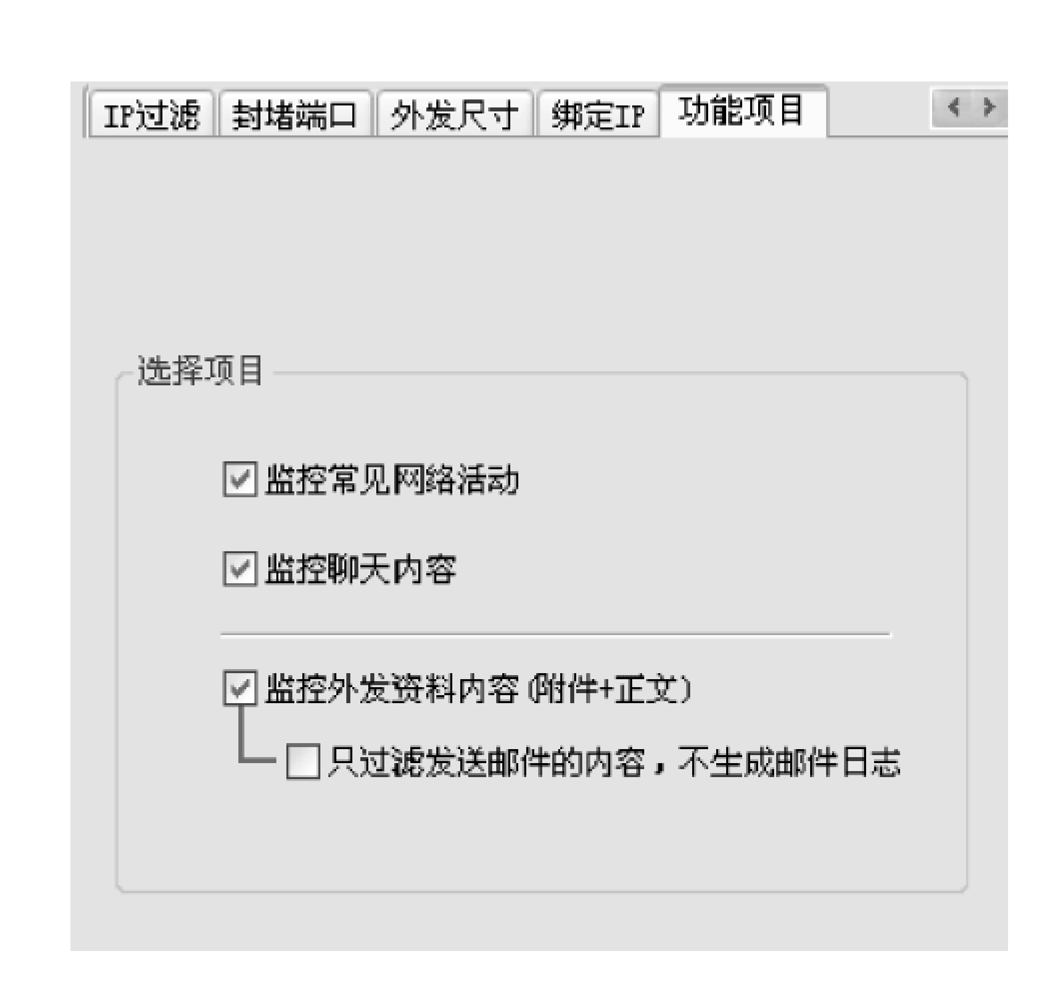


图 11.30　监控项目设置

11.7 日志查阅及日志报表

11.7.1 查阅网络活动日志

(1) 选择目标机器，如图 11.31 所示，在“所有对象”前打上勾，查询日志的时候，是针对所有机器的；相反，如果去掉“所有对象”前面的勾，用户可以随意双击目标机器，以显示对应的日志记录。粗黑显示的机器表明有与其相关的日志记录。

如图 11.31 显示的“机器/账户/IP 地址”是和用户选择的网络监控模式直接关联的，查阅日志的时候，请根据选择的网络监控模式来选择“机器/账户/IP 地址”。

按钮 表示：刷新显示目标机器列表。

按钮 表示：在目标机器列表中查找所要找的目标机器。

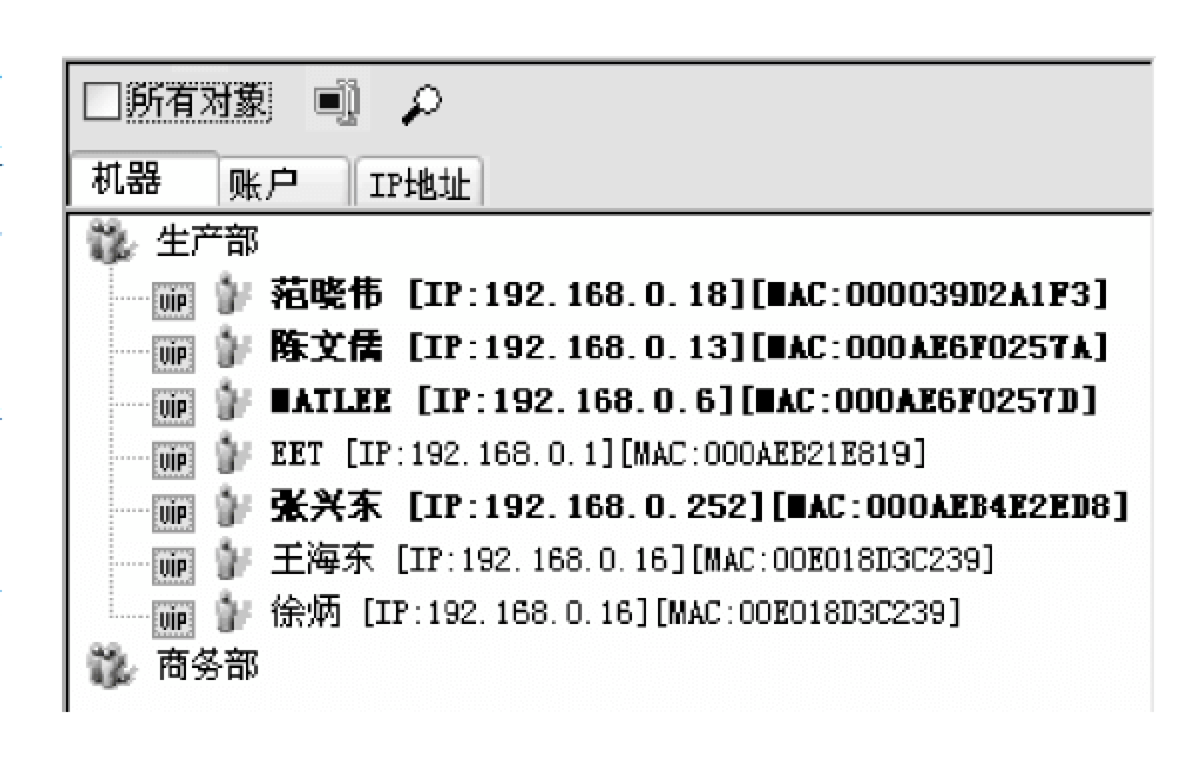


图 11.31　目标机器列表

(2) 选择查询范围，如图 11.32 所示。

“范围”：单击后，弹出快速选择日期



图 11.32　选择查询范围

范围的菜单。

"刷新":更改范围或要查的目标机器后,重新查找并显示对应的日志记录。

小图标表示:将显示的日志内容导出。

小图标表示:查找匹配的日志记录条目。

小图标表示:打印显示的日志内容。

(3) 设置显示的行数,如图 11.33 所示。

(4) 统计日志。针对访问网站的日志和收发邮件的日志,提供简单的统计功能。



图 11.33　显示行数的设置

11.7.2　查阅外发资料日志

(1) 选择目标机器,如图 11.34 所示。上显示的"机器/账户/IP"是和用户选择的网络监控模式直接关联的,查阅日志的时候,请根据选择的网络监控模式来选择"机器/账户/IP 地址"。机器后面的数字直接表明了该机器的日志数量。

(2) 显示日志内容,如图 11.35 所示。

小图标表示是否存在附件。

小图标表示该邮件可直接用 Microsoft Outlook 打开。如果用户发现如图 11.35 下半部分显示乱码,建议用 Outlook 打开。

小图标点后可显示附件。

(3) 搜索邮件,见图 11.36,在输入框中,输入邮箱或关键词时都必须单行输入,对附件类型进行搜索时,如果同时搜索多个类型,那么用逗号分隔开。



图 11.34　外发资料日志



图 11.35　显示日志内容



图 11.36　搜索邮件

11.7.3 日志报表

日志报表分析能提供多种专业图形化报表，同时，在报表结果中，用户也可以查阅详细的日志内容，如图 11.37 所示(在统计数据上双击，可弹出要显示的内容)。



图 11.37　日志报表分析

实验思考题

1. “网路岗”对于网络管理员在日常网络维护上有什么好处？
2. 选择什么样的安装位置有助于“网路岗”获得更加有用的数据？
3. 监控内容如何查阅并保存？
4. “网路岗”能监控的内容中，用处比较大的是哪些？

第12章 实验3 Windows操作系统的安全设置

12.1 实验目的及要求

12.1.1 实验目的

通过实验掌握有效防范攻击的措施、Windows 账户与密码的安全设置、文件系统的保护和加密、安全策略与安全模板的使用、审核和日志的启用、数据的备份好还原、本机漏洞检测软件 MBSA 的使用，建立一个 Windows 操作系统的基本安全框架。

12.1.2 实验要求

根据本教材中介绍的 Windows 操作系统的各项安全性实验要求，详细观察并记录设置前后系统的变化，给出分析报告。

12.1.3 实验设备及软件

1 台安装 Windows 2000/XP 操作系统的计算机，磁盘格式配置为 NTFS，准备 MBSA (Microsoft Baseline Security Analyzer)工具。

12.2 有效的防范攻击措施

12.2.1 计算机常见的被入侵方式

在上网时可能会遇到的入侵方式大概包括以下几种：

(1) 被他人盗取密码；
(2) 系统被木马攻击；
(3) 浏览网页时被恶意的 Java Script 程序攻击；
(4) QQ 被攻击或泄漏信息；
(5) 病毒感染；
(6) 系统存在漏洞使他人攻击自己；
(7) 黑客的恶意攻击。

12.2.2 有效防范攻击的手段

(1) 对于共享资源的设置，如查本地共享资源中是否有不必要的共享，删除不必要的共享，防范 IPC 默认共享等。

(2) 利用 IP 安全策略关闭危险端口，例如 139 端口、445 端口都是病毒常利用的端口。

(3) 管理工具的使用，如本地安全策略、计算机管理、服务、组策略等设置的使用。

(4) 文件加密系统的应用，在 NTFS 格式下的文件及文件夹加密。

(5) 对计算机中重要的文件要及时备份。

(6) 系统扫描工具的使用，如微软公司提供的安全审计工具 MBSA(Microsoft 基准安全分析器)。

12.3　禁止默认共享

1. 什么是默认共享

Windows 2000/XP/2003 版本的操作系统提供了默认共享功能，这些默认的共享都有 $ 标志，意为隐含的，包括所有的逻辑盘(C$、D$、E$ 等)和系统目录(admin$)。

2. 带来的问题

微软的初衷是便于网管进行远程管理，这虽然方便了局域网用户，但对个人用户来说这样的设置是不安全的。如果计算机联网，网络上的任何人都可以通过共享硬盘，随意进入别人的计算机。所以有必要关闭这些共享。Windows XP 在默认安装后允许任何用户通过空用户连接(IPC$)得到系统所有账户和共享列表，任何一个远程用户都可以利用这个空的连接得到目标主机上的用户列表。黑客就利用这项功能，查找系统的用户列表，并使用一些字典工具，对系统进行攻击。这就是网上较流行的 IPC 攻击。

3. 查看本地共享资源

选择"开始"→"运行"中输入 cmd，在命令行窗口中输入 net share，如图 12.1 所示，如果看到有异常的共享，那么应该关闭。但是有时关闭共享后，在下次开机的时候又出现了，那么就应该考虑一下，计算机是否已经被黑客所控制了，或者中了病毒。

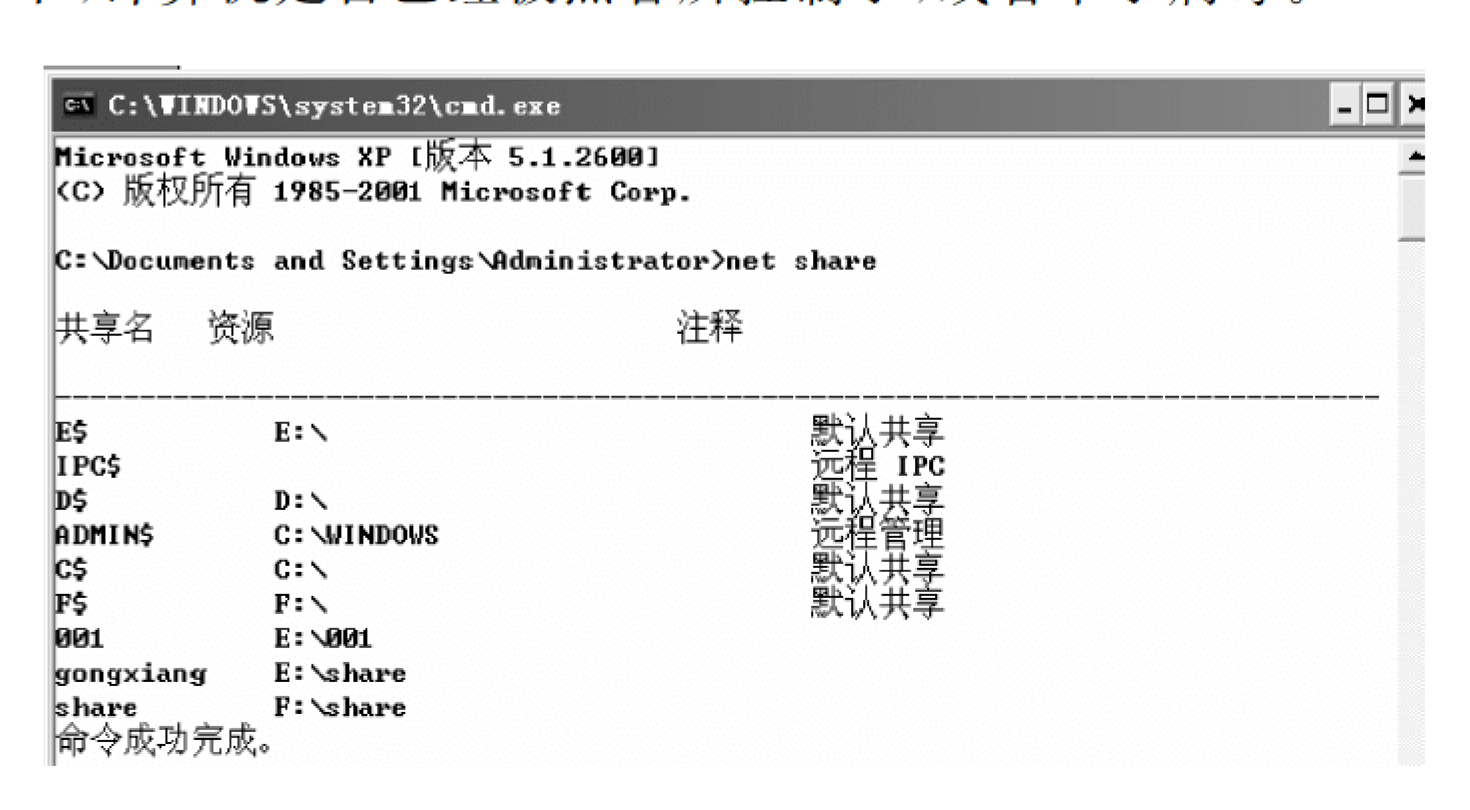


图 12.1　本地共享资源

4. 删除共享(每次输入一个)

net share admin$ /delete

net share c$ /delete

net share d$ /delete

net share e$ /delete

net share f$ /delete

(如果有 g、h 可以继续删除)

5. 注册表改键值法——关闭默认共享漏洞

选择"开始"→"运行",输入 regedit 确定后,打开注册表编辑器,找到 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Service\ lanmanserver\ parameters 项,双击右侧窗口中的 AutoShareServer 项将键值设为 0,这样就能关闭硬盘各分区的共享。如果没有 AutoShareServer 项,可自己新建一个类型为 REG_DWORD,键值为 0 的 DWORD 值。然后还是在这一窗口下再找到 AutoShareWks 项,类型为"REG_DWORD",也将键值设为 0,关闭 admin$ 共享,如图 12.2 所示。

名称	类型	数据
(默认)	REG_SZ	(数值未设置)
AdjustedNullSessionPipes	REG_DWORD	0x00000001 (1)
autodisconnect	REG_DWORD	0x0000000f (15)
AutoShareServer	REG_DWORD	0x00000000 (0)
AutoShareWks	REG_DWORD	0x00000000 (0)
DisableDos	REG_DWORD	0x00000000 (0)
enableforcedlogoff	REG_DWORD	0x00000001 (1)
enablesecuritysignature	REG_DWORD	0x00000000 (0)
Guid	REG_BINARY	75 e0 53 27 22 03 67 42 a7 5e 1c f
Lmannounce	REG_DWORD	0x00000000 (0)
NullSessionPipes	REG_MULTI_SZ	COMNAP COMNODE SQL\QUERY SPOOLSS L
NullSessionShares	REG_MULTI_SZ	COMCFG DFS$
requiresecuritysignature	REG_DWORD	0x00000000 (0)
ServiceDll	REG_EXPAND_SZ	%SystemRoot%\System32\srvsvc.dll
Size	REG_DWORD	0x00000002 (2)
srvcomment	REG_SZ	

图 12.2 修改键值

最后到 HKEY_LOCAL_MACHINE\SYSTEM \CurrentControlSet \Control \Lsa 项处找到 restrictanonymous,将键值设为 1。如果设置为 1,一个匿名用户仍然可以连接到 IPC$ 共享,但限制通过这种连接得到列举 SAM 账号和共享等信息;在 Windows 2000 中增加了 2,限制所有匿名访问除非特别授权,如果设置为 2 的话,可能会有一些其他问题发生,建议设置为 1。如果上面所说的主键不存在,就新建一个再改键值,如图 12.3 所示。

名称	类型	数据
(默认)	REG_SZ	(数值未设置)
auditbaseobjects	REG_DWORD	0x00000000 (0)
Authentication Packages	REG_MULTI_SZ	msv1_0
Bounds	REG_BINARY	00 30 00 00 00 20 00 00
crashonauditfail	REG_DWORD	0x00000000 (0)
disabledomaincreds	REG_DWORD	0x00000000 (0)
everyoneincludesanonymous	REG_DWORD	0x00000000 (0)
fipsalgorithmpolicy	REG_DWORD	0x00000000 (0)
forceguest	REG_DWORD	0x00000000 (0)
fullprivilegeauditing	REG_BINARY	00
ImpersonatePrivilegeUpgradeT...	REG_DWORD	0x00000001 (1)
limitblankpassworduse	REG_DWORD	0x00000001 (1)
lmcompatibilitylevel	REG_DWORD	0x00000000 (0)
LsaPid	REG_DWORD	0x000002a8 (680)
nodefaultadminowner	REG_DWORD	0x00000001 (1)
nolmhash	REG_DWORD	0x00000000 (0)
Notification Packages	REG_MULTI_SZ	scecli
restrictanonymous	REG_DWORD	0x00000001 (1)
restrictanonymoussam	REG_DWORD	0x00000001 (1)
SecureBoot	REG_DWORD	0x00000001 (1)
Security Packages	REG_MULTI_SZ	kerberos msv1_0 schannel wdigest

图 12.3 修改键值

注意：修改注册表后必须重启机器才能生效，但一经改动就会永远停止共享。

12.4 利用 IP 安全策略关闭端口

先看一下如何查看本机打开的端口和 TCP/IP 端口的过滤，选择“开始”→“运行”并输入 cmd，输入命令 netstat -a，如图 12.4 所示。

```
C:\Documents and Settings\Administrator>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    PC-200811211103:epmap  PC-200811211103:0      LISTENING
  TCP    PC-200811211103:microsoft-ds  PC-200811211103:0      LISTENING
  TCP    PC-200811211103:912    PC-200811211103:0      LISTENING
  TCP    PC-200811211103:1025   PC-200811211103:0      LISTENING
  TCP    PC-200811211103:6059   PC-200811211103:0      LISTENING
  TCP    PC-200811211103:9010   PC-200811211103:0      LISTENING
  TCP    PC-200811211103:9011   PC-200811211103:0      LISTENING
  TCP    PC-200811211103:netbios-ssn  PC-200811211103:0      LISTENING
  TCP    PC-200811211103:1025   PC-200811211103:1349   ESTABLISHED
  TCP    PC-200811211103:1026   PC-200811211103:0      LISTENING
  TCP    PC-200811211103:1158   PC-200811211103:1025   CLOSE_WAIT
  TCP    PC-200811211103:1349   PC-200811211103:1025   ESTABLISHED
  TCP    PC-200811211103:netbios-ssn  PC-200811211103:0      LISTENING
  TCP    PC-200811211103:1350   219.238.235.94:http    ESTABLISHED
  TCP    PC-200811211103:netbios-ssn  PC-200811211103:0      LISTENING
  UDP    PC-200811211103:microsoft-ds  *:*
  UDP    PC-200811211103:isakmp  *:*
  UDP    PC-200811211103:4500   *:*
  UDP    PC-200811211103:ntp    *:*
```

图 12.4　开放的端口

1. 关闭自己的 139 端口（IPC 和 RPC 漏洞存在于此）

开启 139 端口虽然可以提供共享服务，但是常常被攻击者所利用进行攻击，比如使用流光、SuperScan 等端口扫描工具，可以扫描目标计算机的 139 端口，如果发现有漏洞，可以试图获取用户名和密码，这是非常危险的。关闭 139 端口的方法是在“网络和拨号连接”中“本地连接”中选取“Internet 协议（TCP/IP）”属性，进入“高级 TCP/IP 设置”“WINS 设置”里面有一项“禁用 TCP/IP 的 NETBIOS”，打勾就关闭了 139 端口，如图 12.5 所示。

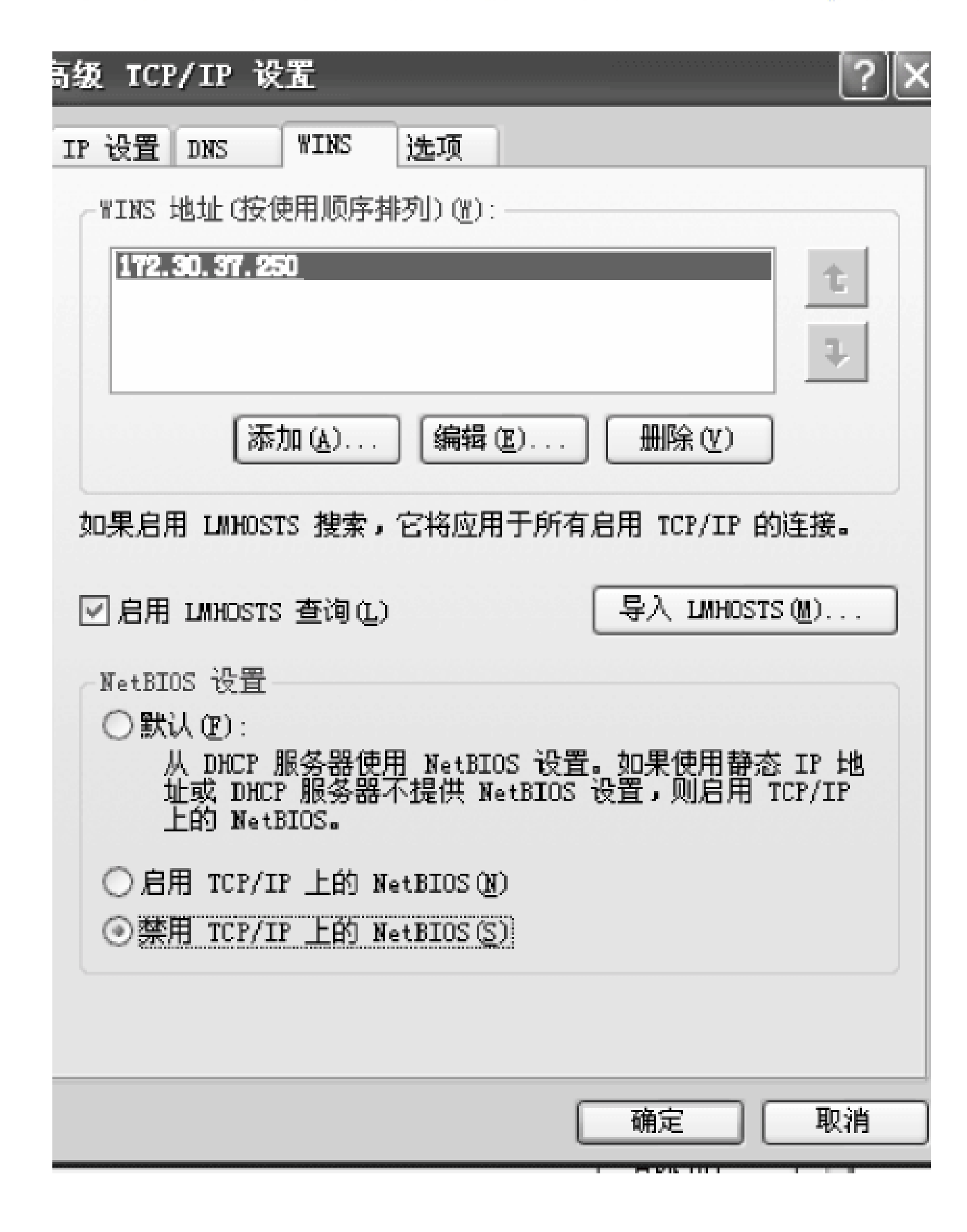


图 12.5　关闭 139 端口

2. 445 端口的关闭

445 端口和 139 端口一起是 IPC $ 入侵的主要通道。通过该端口可以偷偷共享硬盘，甚至会在悄无声息中将硬盘格式化。所以关闭 445 端口是非常必要的，封堵住 445 端口漏洞。修改注册表，添加一个键值 HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NetBT\

Parameters 在右面的窗口建立一个 SMBDeviceEnabled DWORD 值，类型为 REG_DWORD，键值为 0，如图 12.6 所示。

名称	类型	数据
(默认)	REG_SZ	(数值未设置)
BcastNameQueryCount	REG_DWORD	0x00000003 (3)
BcastQueryTimeout	REG_DWORD	0x000002ee (750)
CacheTimeout	REG_DWORD	0x000927c0 (600000)
DhcpNodeType	REG_DWORD	0x00000008 (8)
EnableLMHOSTS	REG_DWORD	0x00000001 (1)
NameServerPort	REG_DWORD	0x00000089 (137)
NameSrvQueryCount	REG_DWORD	0x00000003 (3)
NameSrvQueryTimeout	REG_DWORD	0x000005dc (1500)
NbProvider	REG_SZ	_tcp
SessionKeepAlive	REG_DWORD	0x0036ee80 (3600000)
Size/Small/Medium/Large	REG_DWORD	0x00000001 (1)
TransportBindName	REG_SZ	\Device\
SMBDeviceEnabled	REG_DWORD	0x00000000 (0)

图 12.6　建立键值

3. 禁止终端服务远程控制、远程协助

"终端服务"是 Windows XP 在 Windows 2000 系统(Windows 2000 利用此服务实现远程的服务器托管)上遗留下来的一种服务形式。用户利用终端可以实现远程控制。"终端服务"和"远程协助"是有一定区别的，虽然都实现的是远程控制，终端服务更注重用户的登录管理权限，它的每次连接都需要当前系统的一个具体登录 ID，且相互隔离，并独立于当前计算机用户的邀请，可以独立、自由登录远程计算机。

在 Windows XP 系统下，"终端服务"是被默认打开的，也就是说，如果有人知道你计算机上的一个用户登录 ID，并且知道计算机的 IP，它就可以完全控制你的计算机。

在 Windows XP 系统里关闭"终端服务"的方法如下：右击选择"我的计算机"→"属性"，选择"远程"项，去掉"允许用户远程连接到这台计算机"前面的"√"即可，如图 12.7 所示。

在 Windows XP 上有一项名为"远程协助"的功能，它允许用户在使用计算机发生困难时，向 MSN 上的好友发出远程协助邀请，来帮助自己解决问题。

而这个"远程协助"功能正是"冲击波"病毒所要攻击的 RPC(Remote Procedure Call)服务在 Windows XP 上的表现形式。建议用户不要使用该功能，使用前也应该安装 Microsoft 提供的 RPC 漏洞工具和"冲击波"免疫程序。禁止"远程协助"的方法是：右击选择"我的计算机"→"属性"，选择"远程"项，去掉"允许从这台计算机发送远程协助邀请"前面的"√"即可。

4. 屏蔽闲置的端口

使用系统自带的"TCP/IP 筛选服务"就能够限制端口。方法如下：在"网络连接"上单击右键，选择"属性"，打开"网络连接属性"对话框，在"常规"项里选中里面的"Internet 协议(TCP/IP)"然后单击下面的"属性"按钮，在"Internet 协议(TCP/IP)属性"窗口里，单击下面的"高级"按钮，在弹出的"高级 TCP/IP 设置"窗口里选择"选项"项，再单击下面的"属性"按钮，最后弹出"TCP/IP 筛选"窗口，通过窗口里的"只允许"单选框，分别添加 TCP、UDP、IP 等网络协议允许的端口，如图 12.8 所示，然后添加需要的 TCP 和 UDP 端口就可以了，如果对端口不是很了解的话，不要轻易进行过滤，不然可能会导致一些程序无法使用。未提供各种服务的情况，可以屏蔽掉所有的端口。这是最佳的安全防范形式，但是不适合初学者操作。

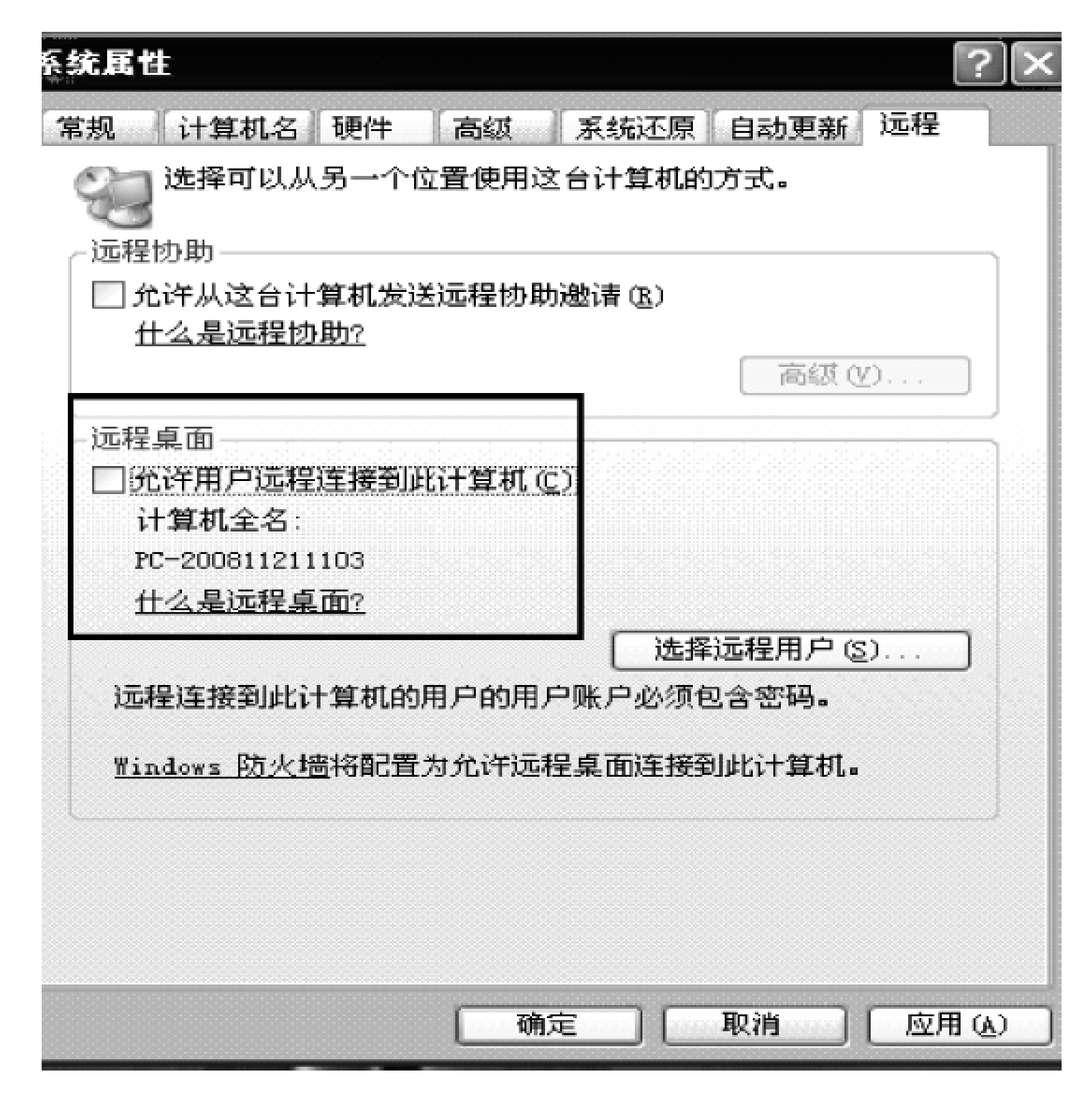


图 12.7　取消远程连接



图 12.8　网络协议允许的端口

12.5　设置策略项,做好内部防御

12.5.1　服务策略——禁用服务

若 PC 没有特殊用途,基于安全考虑,选择"控制面板"→"管理工具"→"服务",如图 12.9 所示。



图 12.9　服务选项

禁用以下服务：

- Alerter(通知所选用户和计算机有关系统管理级警报)。
- ClipBook(启用“剪贴簿查看器”储存信息并与远程计算机共享)。
- Human Interface Device Access(启用对智能界面设备(HID)的通用输入访问，它激活并保存键盘、远程控制和其他多媒体设备上的预先定义的热按钮)。
- IMAPI CD-Burning COM Service(用 Image Mastering Applications Programming Interface 管理 CD 录制)。
- Indexing Service(提供本地或远程计算机上文件的索引内容和属性，泄露信息)。
- Messenger(信使服务)
- NetMeeting Remote Desktop Sharing(使授权用户能够通过使用 NetMeeting 跨企业 intranet 远程访问此计算机)。
- Network DDE(为在同一台计算机或不同计算机上运行的程序提供动态数据交换)。
- Network DDE DSDM(管理动态数据交换(DDE) 网络共享)。
- Print Spooler(将文件加载到内存中以便迟后打印)。
- Remote Desktop Help Session Manager(管理并控制远程协助)。
- Remote Registry(使远程用户能修改此计算机上的注册表设置)。
- Routing and Remote Access(在局域网以及广域网环境中为企业提供路由服务。黑客利用路由服务刺探注册信息)。
- Server(支持此计算机通过网络的文件、打印和命名管道共享)。
- TCP/IP NetBIOS Helper(允许对“TCP/IP 上 NetBIOS(NetBT)”服务以及 NetBIOS 名称解析的支持)。
- Telnet(允许远程用户登录到此计算机并运行程序)。
- Terminal Services(允许多位用户连接并控制一台机器，并且在远程计算机上显示桌面和应用程序)。
- Windows Image Acquisition(WIA)(为扫描仪和照相机提供图像捕获)。

如果发现机器开启了一些很奇怪的服务，如 r_server 这样的服务，必须马上停止该服务，因为这完全有可能是黑客使用控制程序的服务端。

12.5.2 审核策略

审核策略可以帮助用户发现非法入侵者的一举一动，还可以作为用户将来追查黑客的依据。

选择“管理工具”→“本地安全设置”→“本地策略”→“审核策略”，把审核策略设置为如图 12.10 所示的内容。

然后再选择“管理工具”→“事件查看器”。

应用程序：通过右击选择“属性”来设置日志大小上限，设置了 512 000KB，选择不改写事件。

安全性：通过右击选择“属性”来设置日志大小上限，设置了 512 000KB，选择不改写事件。

系统：通过右击选择“属性”来设置日志大小上限，设置了 512 000KB，选择不改写事件。

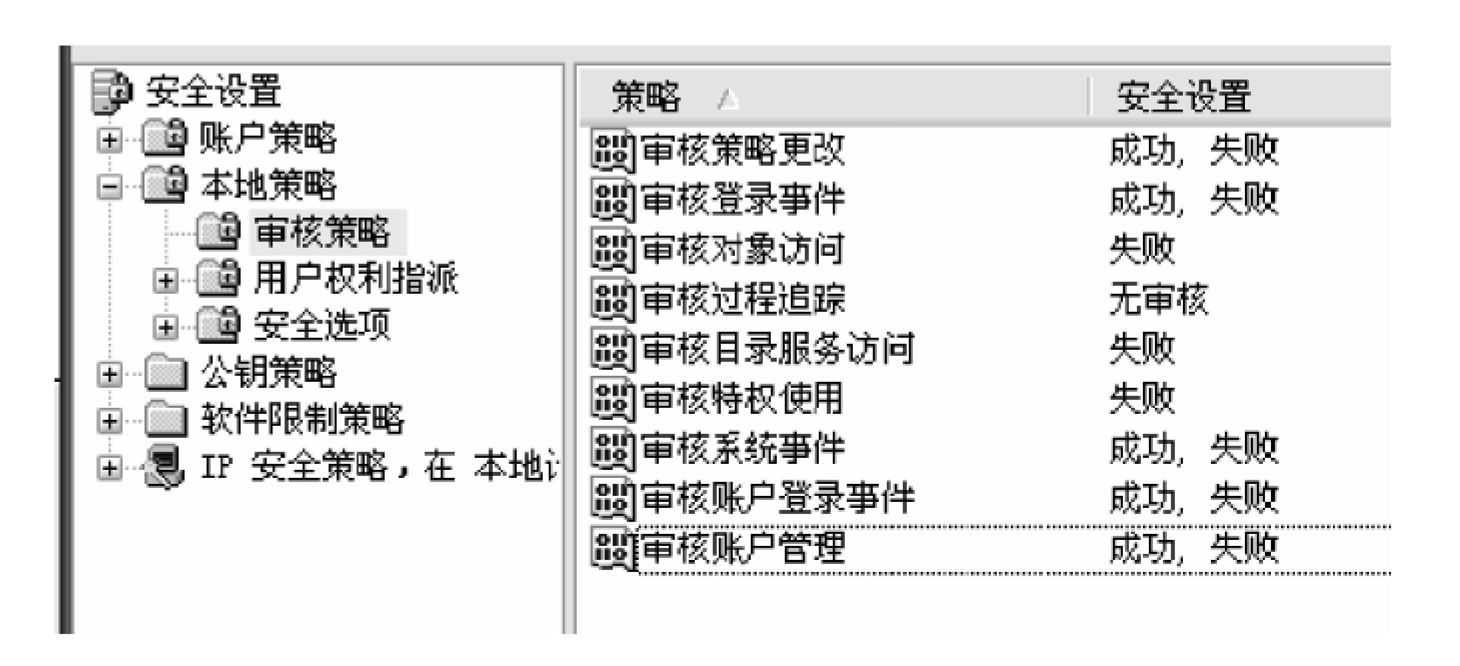


图 12.10　审核策略设置

12.5.3　安全选项

安全选项是作为增强 Windows 安全的最佳做法，同时也为攻击者设置更多的障碍以减少对 Windows 的攻击的重要系统安全工具，在"本地策略"→"安全选项"中进行如下设置：

- 交互式登录：不显示上次的用户名(设置为启用)。
- 网络访问：不允许 SAM 账户的匿名枚举(设置为"启用")。
- 网络访问：让"每个人"权限应用于匿名用户(设置为关闭)。
- 网络访问：可匿名的共享(将后面的值删除)。
- 网络访问：可匿名的命名管道(将后面的值删除)。
- 网络访问：可远程访问的注册表路径(将后面的值删除)。
- 网络访问：可远程访问的注册表的子路径(将后面的值删除)。
- 网络访问：限制匿名访问命名管道和共享(将后面的值删除)。
- 网络安全：不要在下次更改密码时存储 LAN Manager 的 Hash 值(设置为"启用")。
- 关机：清除虚拟内存页面文件(设置为"启用")。
- 关机：允许在未登录前关机(设置为"关闭")。
- 账户：重命名系统管理员账户(确定一个新名字)。
- 账户：重命名来宾账户(确定一个新名字)。

12.5.4　启用安全模板

启用前，请记录当前系统的账户策略和审核日志状态，以便于同实验后的设置进行比较。

(1) 选择"开始"→"运行"，在对话框中输入 mmc，打开系统控制台。

(2) 选择工具栏上"控制台"，在弹出的菜单中选择"添加/删除管理单元"，单击"添加"按钮，在弹出的窗口中分别选择"安全模板"、"安全设置和分析"，单击"添加"按钮后关闭窗口，再单击"确定"按钮，如图 12.11 所示。

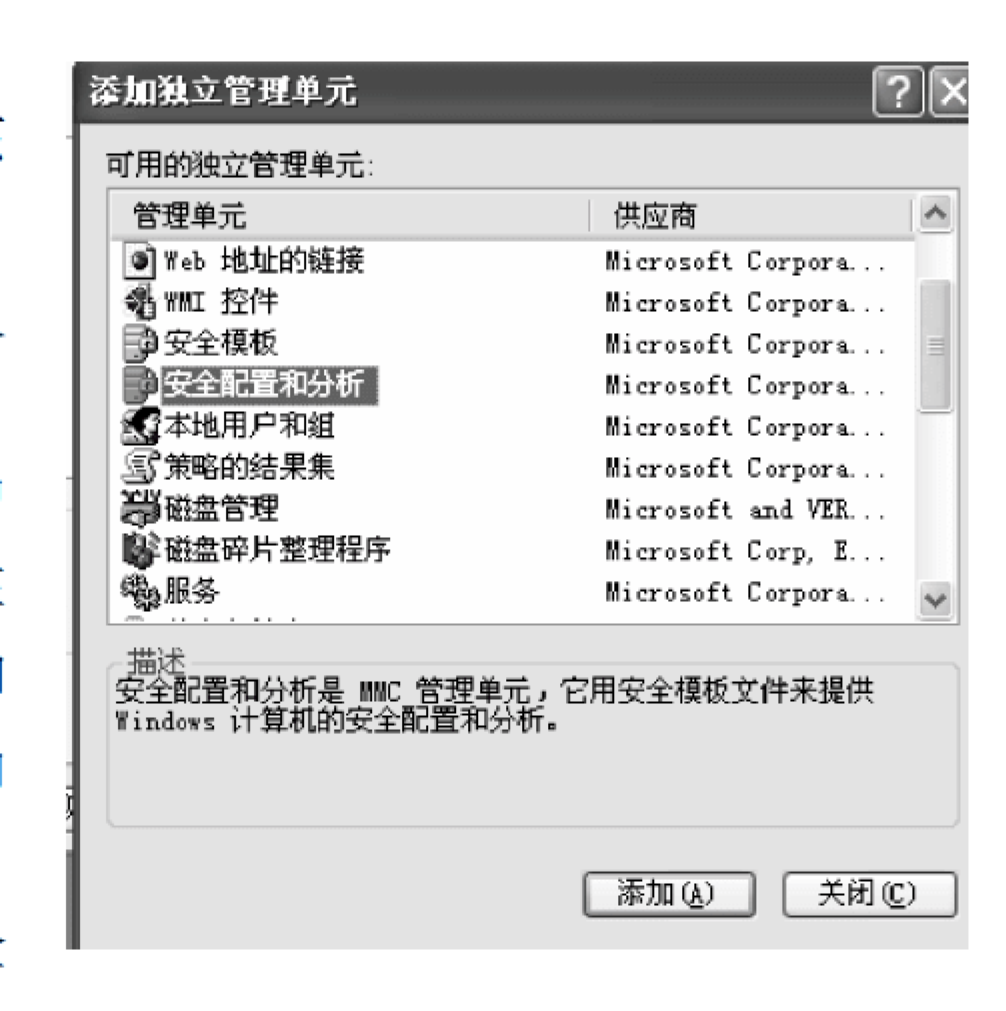


图 12.11　添加控制模块

(3) 此时系统控制台中根节点下添加了"安全模板"、"安全设置分析"两个文件夹，打开"安全模

板”文件夹，可以看到系统中存在的安全模板，如图 12.12 所示。右击模板名称，选择“设置描述”，可以看到该模板的相关信息。选择“打开”，右侧窗口出现该模板的安全策略，双击每个安全策略可看到其相关配置。



图 12.12　安全模板

(4) 右击“安全设置与分析”，选择“打开数据库”。在弹出的对话框中输入预建安全数据库的名称，例如起名为 mycomputer.sdb，单击“打开”按钮，在弹出的窗口中，根据计算机准备配置成的安全级别，选择一个安全模板将其导入。

(5) 右击“安全设置与分析”，选择“立即分析计算机”，单击“确定”按钮，系统开始按照上一步中选定的安全模板，对当前系统的安全设置是否符合要求进行分析，将分析结果记录在实验报告中。

(6) 右击“安全设置与分析”，选择“立即配置计算机”，则按照第(4)步中所选的安全模板的要求对当前系统进行配置。

(7) 在实验报告中记录实验前系统的默认配置，接着记录启用安全模板后系统的安全设置，记录下比较和分析的结果。

12.5.5　新建安全模板

(1) 展开“安全模板”，右击模板所在路径，选择“新加模板”，在弹出的对话框中输入预加入的模板名称 mytem，在“安全模板描述”中填入“自设模板”。查看新加模板是否出现在模板列表中。

(2) 双击 mytem，在现实的安全策略列表中双击“账户策略”下的“密码策略”，可发现其中任一项均显示“没有定义”，双击预设置的安全策略(如“密码长度最小值”)。

(3) 在“在模板中定义这个策略设置”前打勾，在框中填入密码的最小长度为 7。

(4) 依次设定“账户策略”、“本地策略”等项目中的每项安全策略，直至完成安全模板的设置。

12.5.6　用户权利指派策略

打开“管理工具”→“找到本地安全设置”→“本地策略”→“用户权利指派”，如图 12.13 所示。

(1) “从网络访问此计算机”里面一般默认有 5 个用户，除 Administrators 外删除 4 个，当然，接下来还得创建一个属于自己的 ID。

(2) 从远程系统强制关机，Admin 账户也删除，一个都不留。



图 12.13　用户权利指派

（3）拒绝从网络访问这台计算机，将 ID 删除。

（4）从网络访问此计算机，Admin 也可删除，如果你不使用类似 3389 服务。

（5）允许通过终端服务登录。Admin 账户也删除，一个都不留。

12.5.7　账户锁定策略

为了防止他人进入计算机时反复猜测密码进行登录，可以锁定无效登录，当密码输入错误达设定次数后，便锁定此账户，在一定时间内不能再以该账户登录。

选择“本地安全设置”→“账户策略”→“账户锁定策略”，打开“账户锁定阈值”对话框，设置 3 次无效登录就锁住账号，如图 12.14 所示。

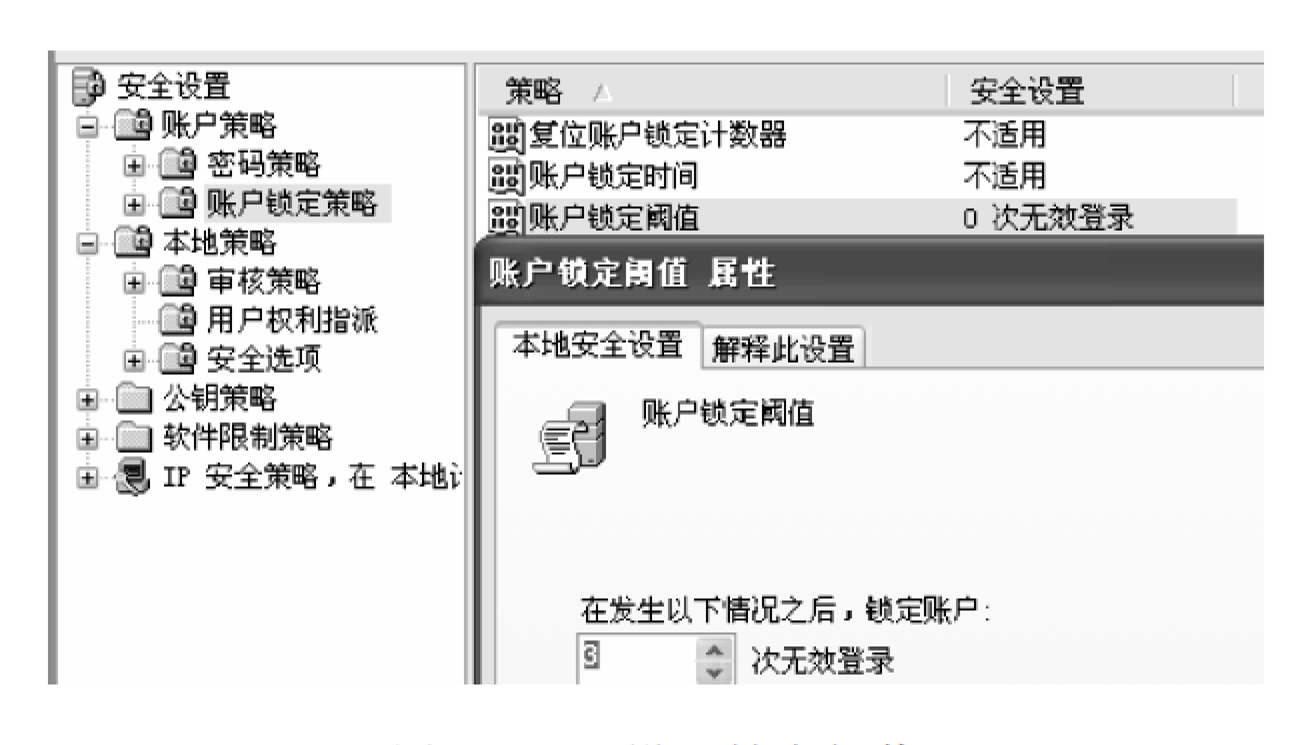


图 12.14　设置锁定阈值

复位账户锁定计数器（确定 30 分钟以后），确定（账户锁定时间 30 分钟），如图 12.15 所示。

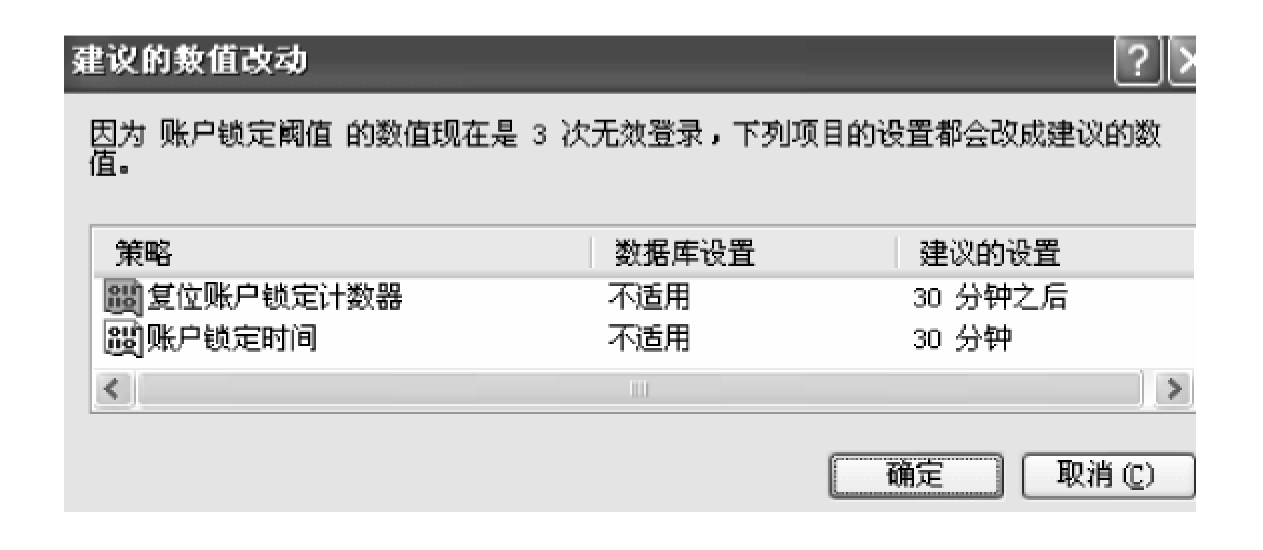


图 12.15　锁定计数器与时间

12.5.8 用户策略

选择“管理工具”→“计算机管理”→“本地用户和组”→“用户”，如图 12.16 所示。



图 12.16 删除用户

删除 Support_388945a0 用户等。只留下更改好名字的 administrator 权限。

12.5.9 关闭自动运行功能

(1) 执行“开始”→“运行”菜单命令，输入 gpedit. msc，并运行，打开“组策略”窗口。

(2) 在左栏的“本地计算机策略”下，打开“计算机配置”→“管理模板”→“系统”，然后在右栏的“设置”标题下，双击“关闭自动播放”，如图 12.17 所示。

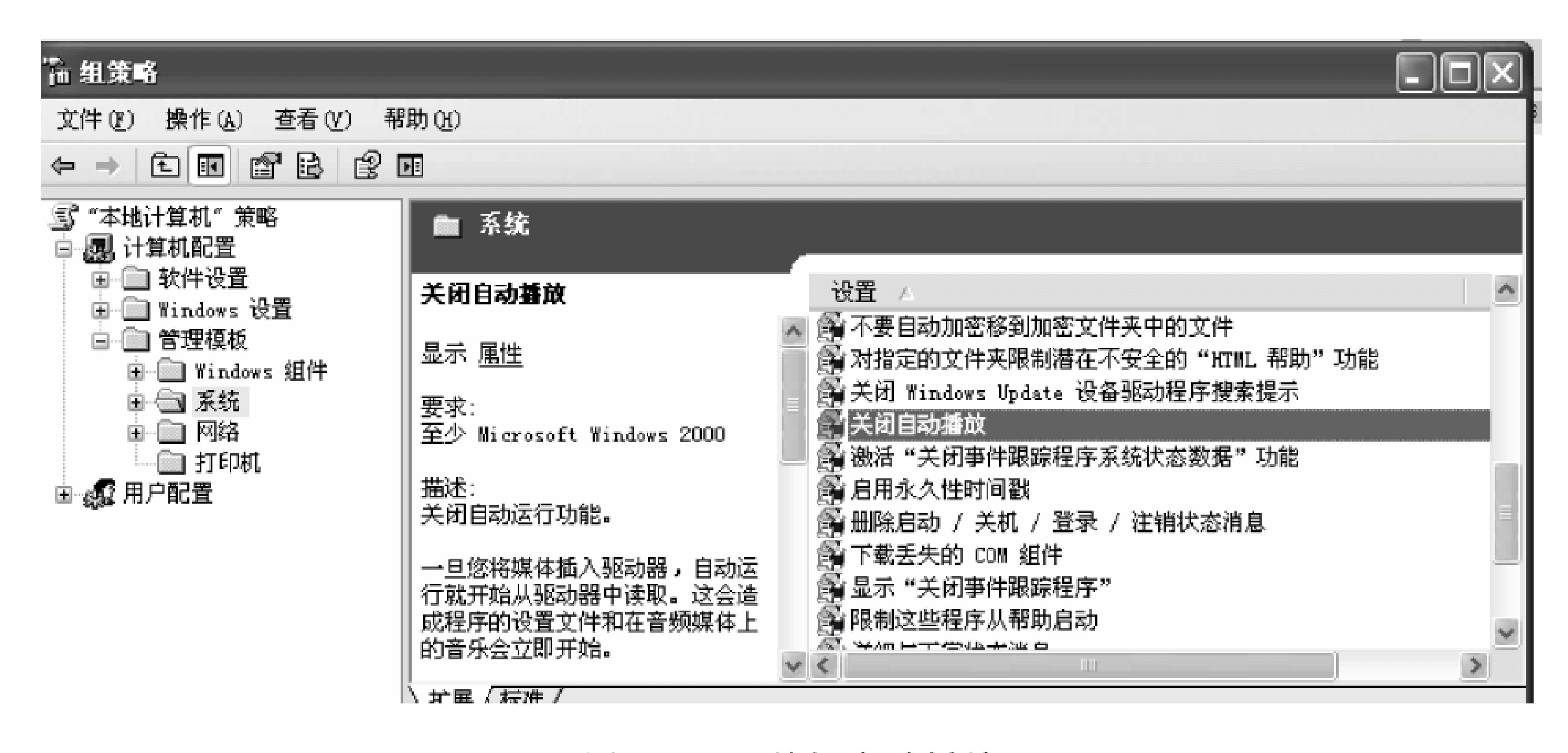


图 12.17 关闭自动播放

(3) 选择“设置”选项卡，选取“已启用”复选按钮，然后在“关闭自动播放”框中选择“所有驱动器”，单击“确定”按钮，退出“组策略”窗口，如图 12.18 所示。



图 12.18 启动服务

在“用户配置”中同样也可以定制这个“关闭自动播放”。但“计算机配置”中的设置比“用户配置”中的设置范围更广。有助于多个用户都使用这样的设置。

12.6 文件加密系统

每个人都有一些不希望别人看到的东西，例如学习计划、情书等，大家都喜欢把它们放在一个文件夹里，采用 Windows 自带的文件夹加密功能来实现对文件加密，NTFS 是 WinNT 以上版本支持的一种提供安全性、可靠性的高级文件系统。在 Win2000 和 WinXP 中，NTFS 提供诸如文件和文件夹加密的高级功能。

12.6.1 加密文件或文件夹

(1) 打开 Windows 资源管理器。

(2) 右击要加密的文件或文件夹，然后选择“属性”。

(3) 在“常规”选项卡上，单击“高级”选项。选中“加密内容以便保护数据”复选框，如图 12.19 所示。



图 12.19　加密选项

在加密过程中还要注意以下几点：

(1) 只可以加密 NTFS 分区卷上的文件和文件夹，FAT 分区卷上的文件和文件夹无效。

(2) 被压缩的文件或文件夹也可以加密。如果要加密一个压缩文件或文件夹，则该文件或文件夹将会被解压。

(3) 无法加密标记为“系统”属性的文件，并且位于操作系统根目录结构中的文件也无法加密。

(4) 在加密文件夹时，系统将询问是否要同时加密它的子文件夹。如果选择是，那它的子文件夹也会被加密，以后所有添加进文件夹中的文件和子文件夹都将在添加时自动加密。

加密后用不同用户登录计算机，查看加密文件是否能够打开。

12.6.2 备份加密用户的证书

用户对文件的加密后，在重装系统或删除用户前一定要备份加密用户的证书，否则重装

系统或删除用户后加密文件将无法被访问。

(1) 以加密用户登录计算机。

(2) 执行“开始”→“运行”菜单命令，输入 mmc，然后单击“确定”按钮。

(3) 在“控制台”菜单上，单击“添加/删除管理单元”，然后单击“添加”按钮。

(4) 在“单独管理单元”下，选择“证书”，然后单击“添加”按钮，如图 12.20 所示。

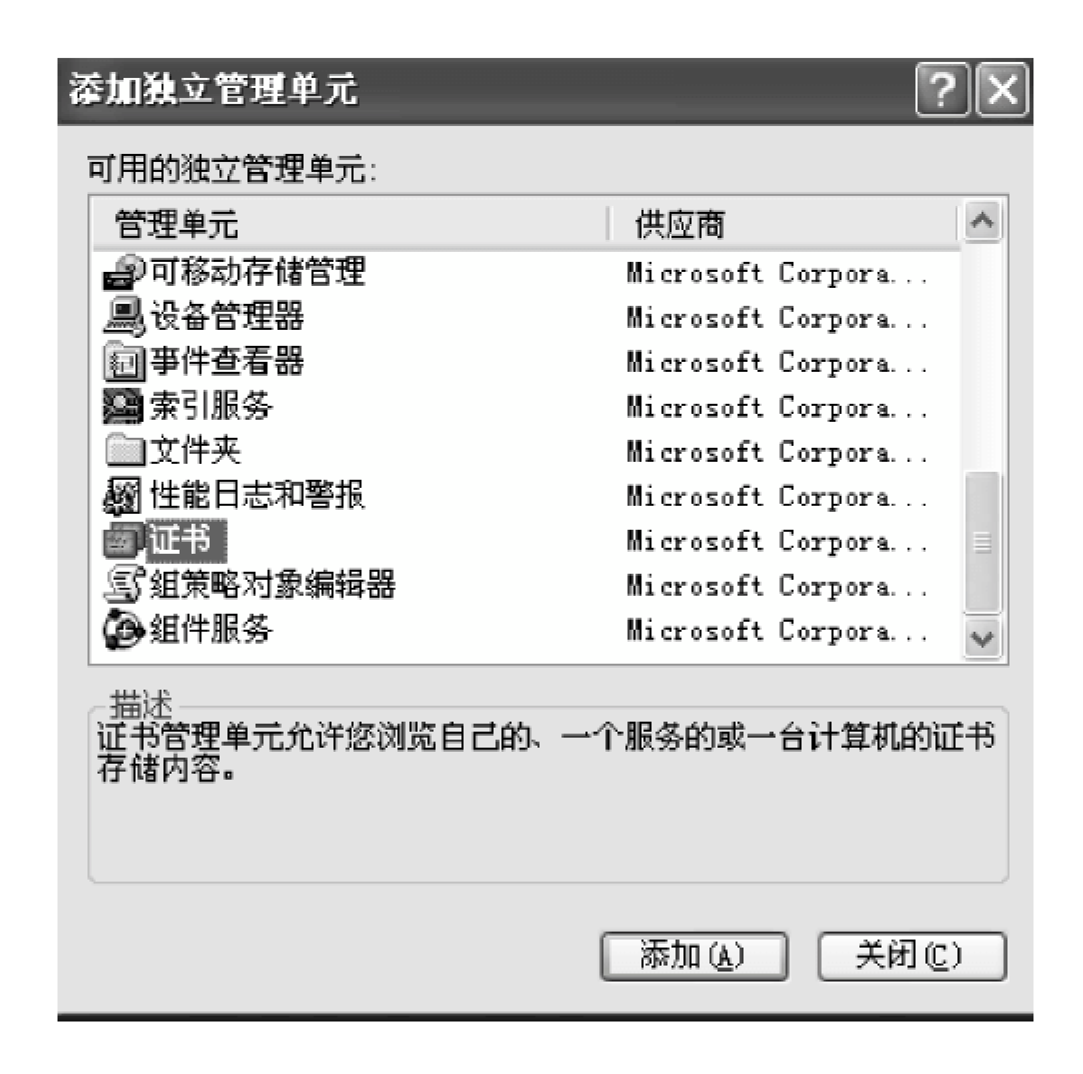


图 12.20　添加证书模块

(5) 选择“我的用户账户”，然后单击“完成”按钮。

(6) 单击“关闭”按钮，然后单击“确定”按钮。

(7) 双击“证书——当前用户”选项，双击“个人”选项，然后双击“证书”选项，如图 12.21 所示。

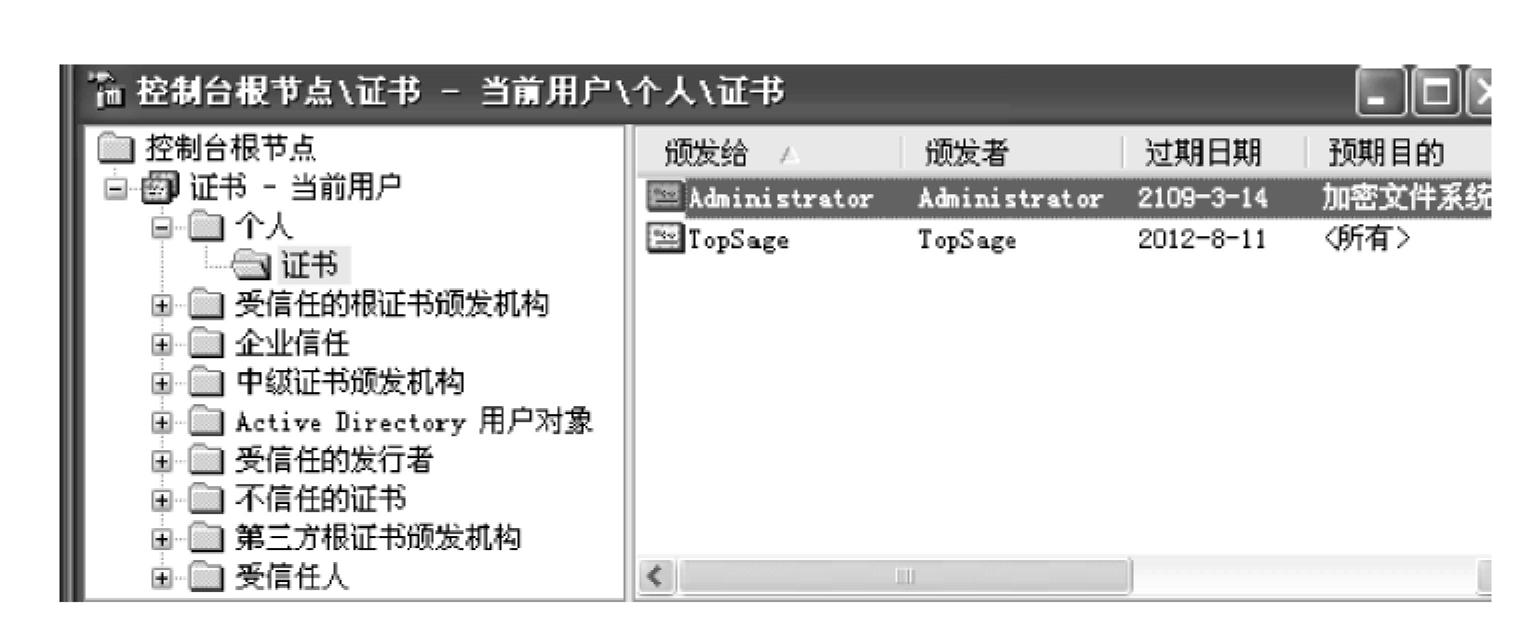


图 12.21　显示加密证书

(8) 单击“预期目的”栏中显示“加密文件”字样的证书。

(9) 右击该证书，指向“所有任务”，然后单击“导出”按钮，如图 12.22 所示。

(10) 按照证书导出向导的指示将证书及相关的私钥以 PFX 文件格式导出(注意：推荐使用“导出私钥”方式导出，如图 12.23 所示，这样可以保证证书受密码保护，以防别人盗用。另外，证书只能保存到你有读写权限的目录下)。

(11) 保存好证书，将 PFX 文件保存好。以后重装系统之后无论在哪个用户下只要双击这个证书文件，导入这个私人证书就可以访问 NTFS 系统下由该证书的原用户加密的文件夹。

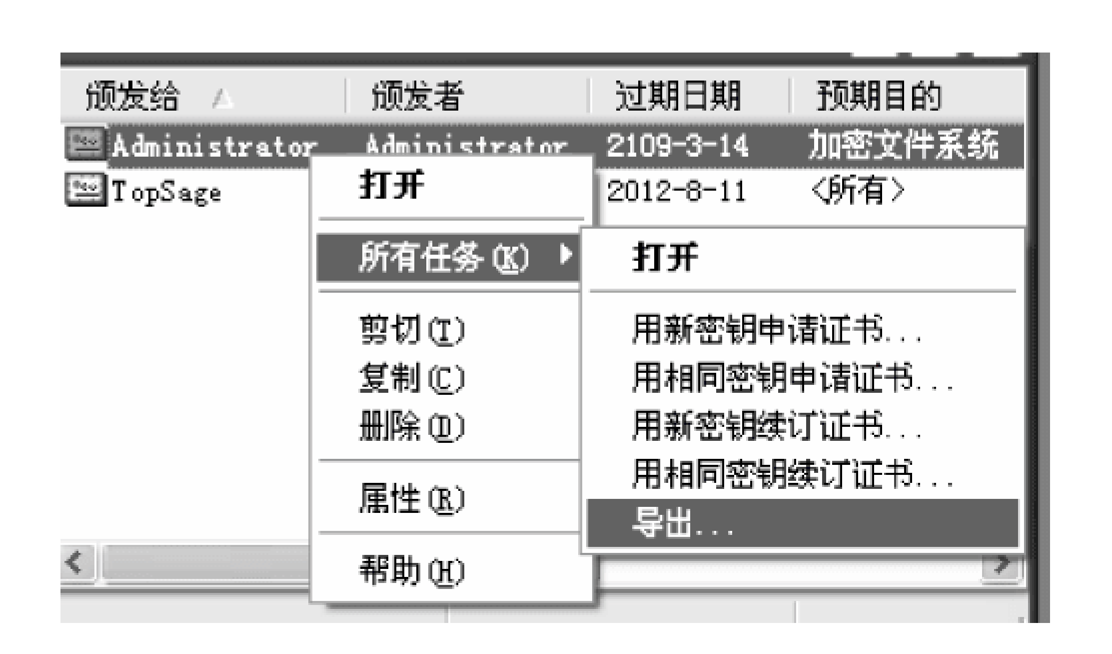


图 12.22　导出证书



图 12.23　导出私钥

最后要提一下，这个证书还有下述用途。

① 给予不同用户访问加密文件夹的权限：将我的证书按“导出私钥”方式导出，将该证书发给需要访问这个文件夹的本机其他用户。然后由其他用户登录，导入该证书，实现对这个文件夹的访问。

② 在其他 WinXP 机器上对用“备份恢复”程序备份的以前的加密文件夹的恢复访问权限，将加密文件夹用“备份恢复”程序备份，然后把生成的 Backup.bkf 连同这个证书拷贝到另外一台 WinXP 机器上，用“备份恢复”程序将它恢复出来（注意：只能恢复到 NTFS 分区）。然后导入证书，即可访问恢复出来的文件了。

12.7　文件和数据的备份

为了保护服务器，用户应该安排对所有数据进行定期备份。建议安排对所有数据（包括服务器的系统状态数据）进行每周普通备份。普通备份将复制您选择的所有文件，并将每个文件标记为已备份。此外，还建议安排进行每周差异备份。差异备份复制自上次普通备份以来创建和更改的文件。

12.7.1　安排进行每周普通备份

(1) 执行“开始”→“运行”菜单命令，输入 ntbackup，然后单击“确定”按钮，此时会出现“备份或还原向导”，单击“下一步”按钮。

(2) 在“备份或还原向导”页面中，确保已选择“备份文件和设置”，然后单击“下一步”按钮，在“要备份的内容”页面中，选择“让我选择要备份的内容”，然后单击“下一步”按钮。

(3) 在“要备份的项目”页面上，单击项目以展开其内容。选择包含应该定期备份的数据的所有设备或文件夹的复选框，然后单击“下一步”按钮，如图 12.24 所示。

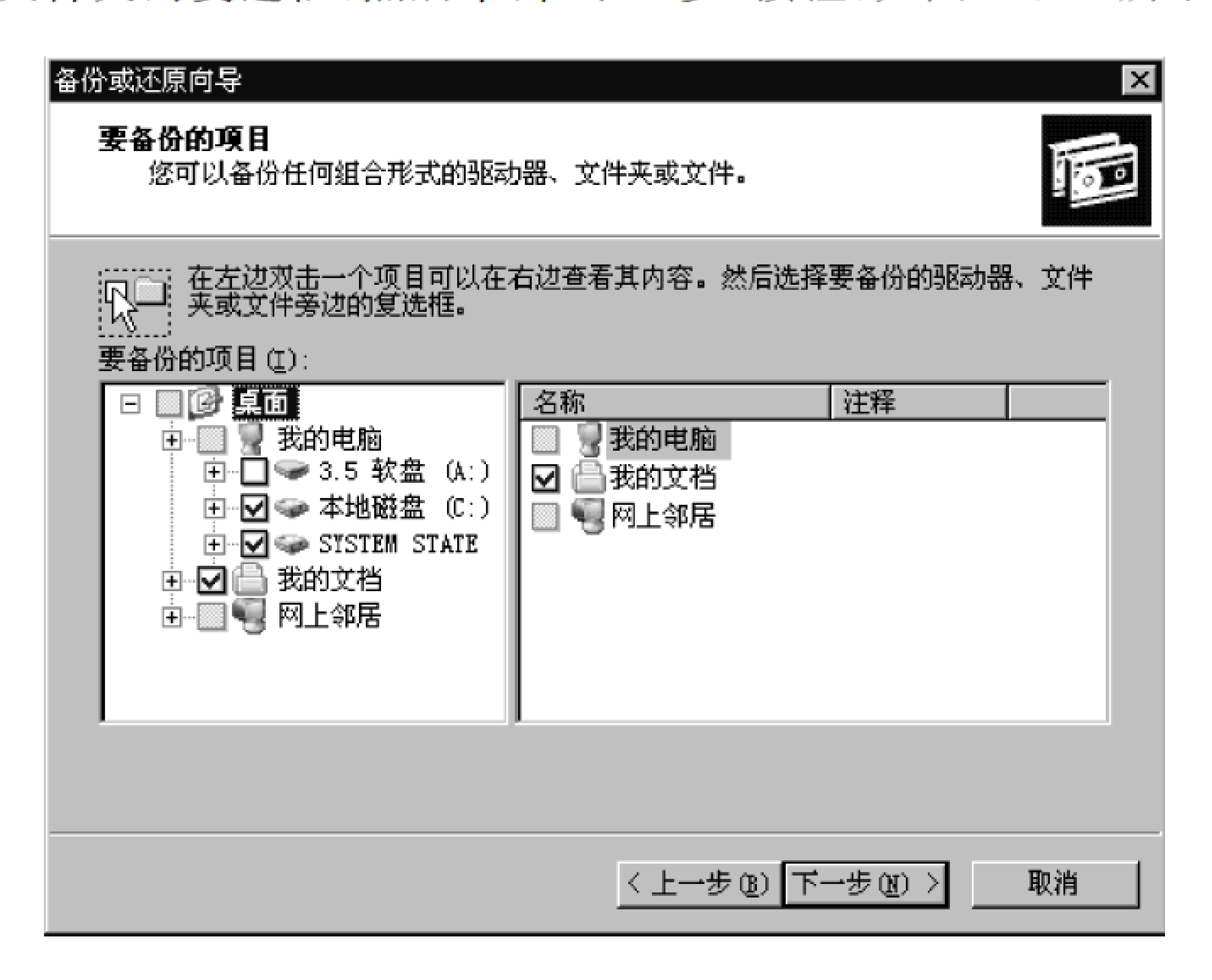


图 12.24　备份的项目

(4) 在“备份类型、目标和名称”页面中的“选择保存备份的位置”中，单击下拉菜单或单击“浏览”以选择保存备份的位置。在“输入这个备份的名称”中，为该备份输入一个描述性名称，然后单击“下一步”按钮，如图 12.25 所示。



图 12.25　备份类型、目标和名称

(5) 在“完成备份或还原向导”页面中，单击“高级”选项，在“备份类型”页面的下拉菜单中选择“正常”，然后单击“下一步”按钮，如图 12.26 所示。

(6) 在“如何备份”页面中选择“备份后验证数据”复选框，然后单击“下一步”按钮，在“备份选项”页面中，确保选择了“将这个备份附加到现有备份”选项，然后单击“下一步”按钮，如图 12.27 所示。



图 12.26　备份类型



图 12.27　备份选项

(7) 在“备份时间”页面中的“什么时候执行备份”下，选择“以后”。在“计划项”的“作业名”中输入描述性名称，然后单击“设定备份计划”按钮，如图 12.28 所示。

(8) 选择“计划作业”对话框的“计划任务”，下拉菜单中的“每周”。在“开始时间”中，使用向上和向下箭头键选择开始备份的适当时间。单击“高级”选项以指定计划任务的开始日期和结束日期，或指定计划任务是否按照特定时间间隔重复运行。在“每周计划任务”中，根据需要选择一天或几天以创建备份，然后单击“确定”按钮，如图 12.29 所示。

(9) 在“设置账户信息”对话框的“运行方式”中，输入域、工作组和已授权执行备份和还原操作的账户的用户名。使用 domain \ username 或 workgroup \ username 格式。在“密码”中输入用户账户的密码。在“确认密码”中再次输入密码，然后单击“确定”按钮，如图 12.30 所示。在“完成备份或还原向导”页面中，确认设置，然后单击“完成”按钮。



图 12.28　备份时间

计划作业
日程安排
设置
从 2004-10-5 起，每周的星期六，1:00
计划任务(S):
每周
开始时间(T):
1:00
高级(V)...
每周计划任务
每(E) 1 周，在:
星期一
星期二
星期三
星期四
星期五
星期六
星期日
显示多项计划(M)。
确定
取消

图 12.29　计划作业

设置账户信息
运行方式(U):
DOMAIN\username
密码(P):
****
确认密码(C):
****
确定
取消

图 12.30　设置账户信息

12.7.2 安排进行每周差异备份

操作步骤与普通备份基本相同，只是在“备份类型”页面的选择要执行的备份操作类型中，选择“差异”，然后单击“下一步”按钮，如图 12.31 所示。



图 12.31 差异备份

12.7.3 从备份恢复数据

(1) 单击“开始”按钮，然后单击“运行”按钮，输入 ntbackup，然后单击“确定”按钮，此时会出现“备份或还原向导”。单击“下一步”按钮。

(2) 在“备份或还原”页面中，单击“还原文件和设置”，然后单击“下一步”按钮。在“还原项目”页面上，单击项目以展开其内容。选择包含要还原的数据的所有设备或文件夹，然后单击“下一步”按钮，如图 12.32 所示。



图 12.32 还原项目

(3) 在“完成备份或还原向导”页面中，如果您要更改任何高级还原选项，例如还原安全设置和交接点数据，请单击“高级”选项。完成设置高级还原选项后，单击“确定”按钮。验证是否所有设置都正确，然后单击“完成”按钮。

12.8 利用 MBSA 检查和配置系统安全

MBSA(Microsoft 基准安全分析器)是微软公司提供的安全审计工具，MBSA Version 1.2 包括可执行本地或远程 Windows 系统扫描的图形和命令行界面。MBSA 运行在 Windows 2000 和 Windows XP 系统上，可以扫描系统以发现常见的系统配置错误，MBSA 可以从微软免费下载，其安装过程也非常简单，按照提示一步步安装即可。下面对 MBSA 的使用方法进行介绍。

下载地址：http://www.microsoft.com/china/technet/security/tools/mbsahome.mspx#EBB。

检查系统漏洞的步骤如下：

(1) 双击打开 MBSA，在弹出的窗口中选择 Scan a computer，如图 12.33 所示。

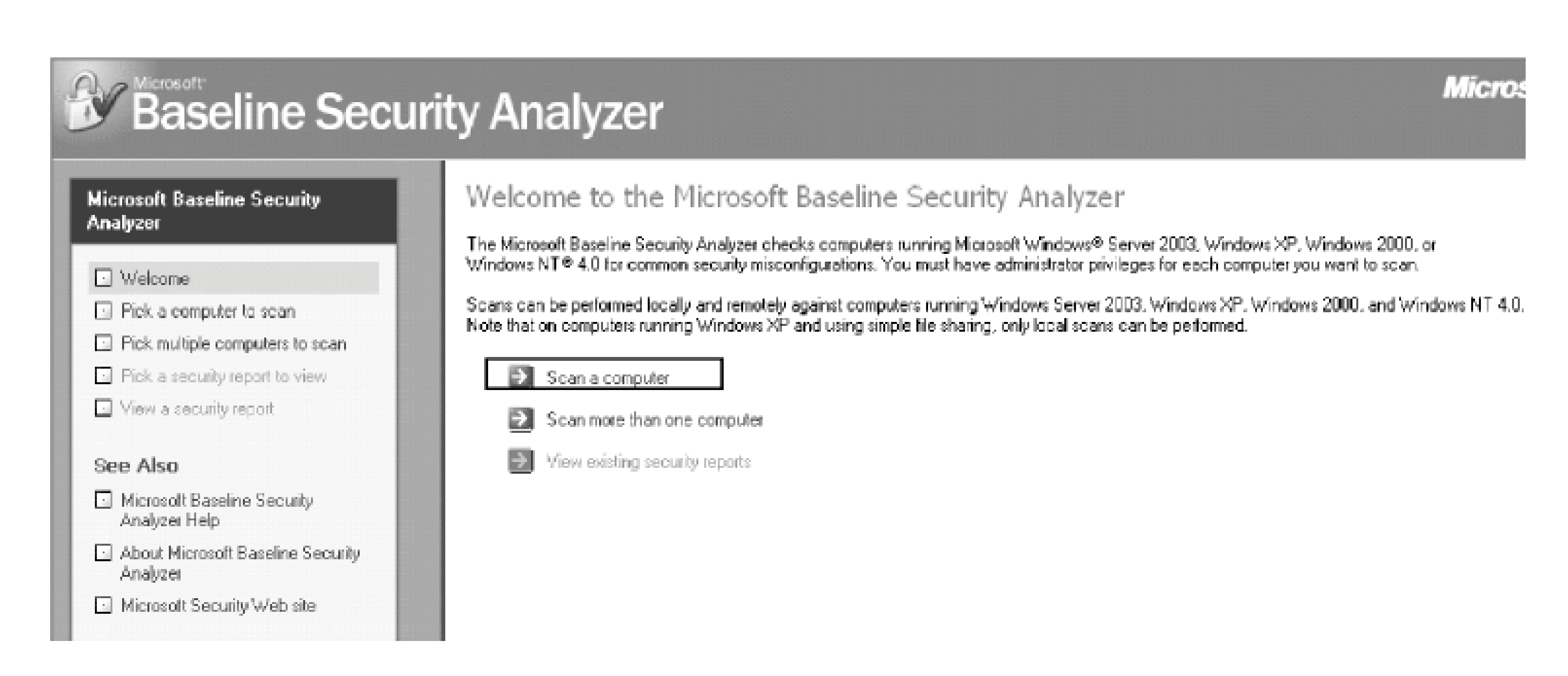


图 12.33 扫描计算机

(2) 在弹出的窗口中填写本地计算机名称或者 IP 地址，并选择希望扫描的漏洞类型。这里采用全部漏洞扫描，单击 start scan 按钮，扫描计算机。

注意：由于扫描过程中需要连接 Microsoft 网站，因此需要事先配置好网络。

(3) 扫描完成后，在实验报告中记录扫描结果。

(4) 查看安全性报告并手动修复漏洞。

安全性报告中，最左侧一览为评估报告，其中红色和黄色的叉号表示该项目未能通过测试；雪花图标表示该项目还可以进行优化，也可能是程序跳过了其中的某项设置；感叹号表示尚有更详细的信息；绿色的对勾表示该项目已通过测试；What was scan 表明检查的项目，result scan 中详细地说明了该项目中出现的问题，how to correct this 说明了解决的方式，如图 12.34 所示。

① 首先查看报告中评估结果为叉号的项目(这里选择 file system)，打开 result detail，查看该项检查中出现的具体问题，如图 12.35 所示。

② 单击 how to correct this 按钮，弹出的窗口显示了有关如何修改项目设置的提示信息。根据提示，我们可以修改不符合安全性要求的设置。

③ 完成修改后，再次进行扫描，查看修改后的设置是否已经达到安全要求。

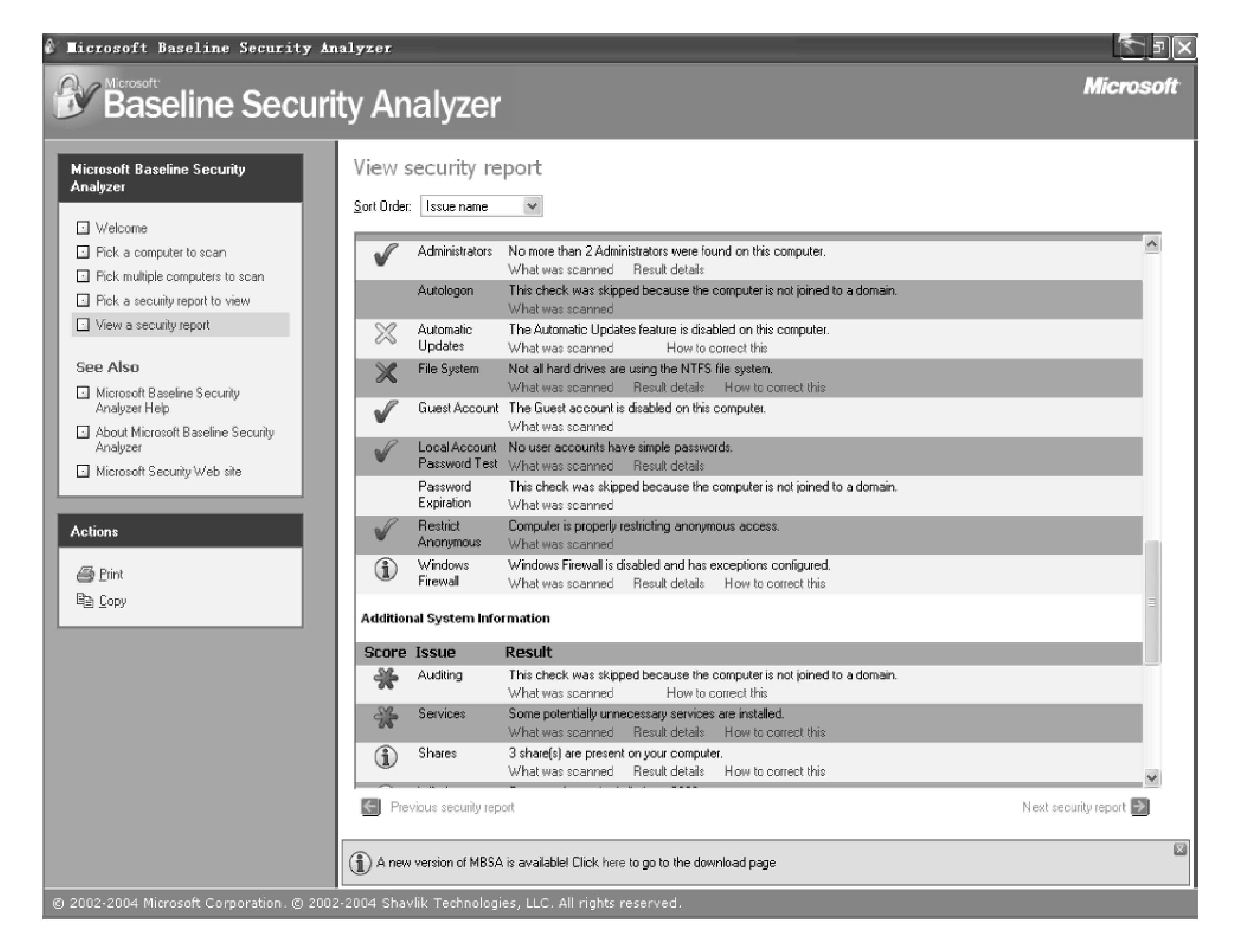


图 12.34 扫描报告

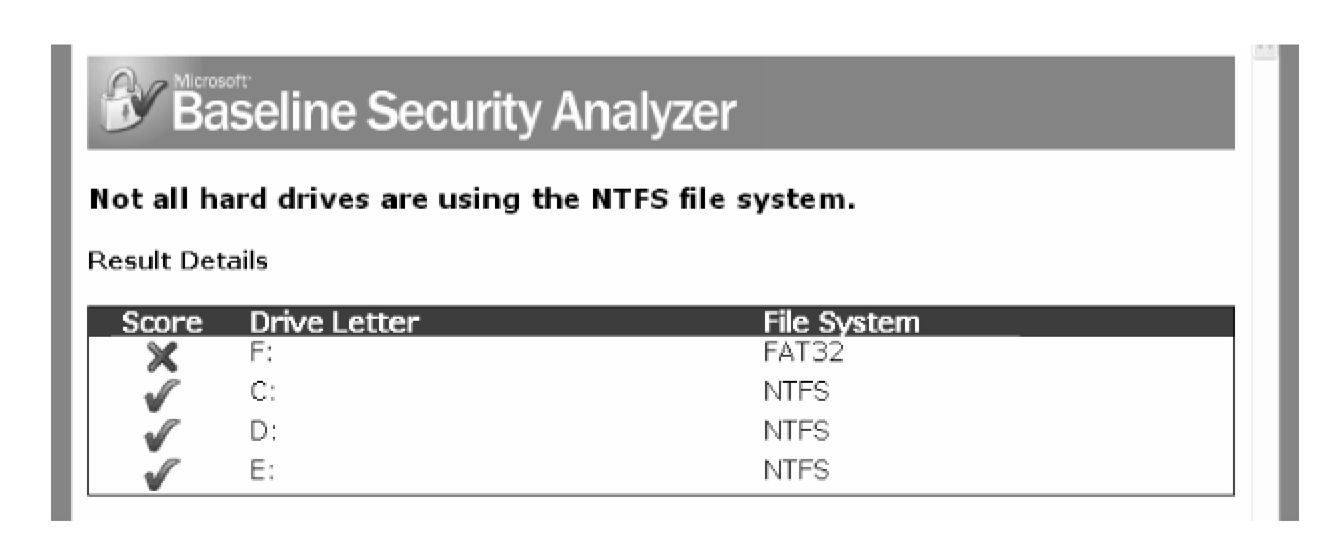


图 12.35 扫描问题

实验思考题

1. 计算机中常用服务都使用了哪些端口?
2. 如何建立一个相对比较安全的共享?
3. 如何根据网络环境不同快速调整安全策略?
4. 加密证书如何保存才会安全?
5. 计算机中哪些数据需要定期备份?
6. 漏洞扫描工具有什么作用?

第 13 章　实验 4　PGP 软件的安装与使用

13.1　实验目的及要求

13.1.1　实验目的

通过实验操作掌握 PGP 软件的安装与基本功能使用、对于加密软件的原理具有一定的了解。能够实现常用的加密功能。

13.1.2　实验要求

根据教材中介绍的 PGP 软件的功能和步骤来完成实验，在掌握基本功能的基础上，实现日常加密应用，给出实验操作报告。

13.1.3　实验设备及软件

2 台安装 Windows 2000/XP 操作系统的计算机，磁盘格式配置为 NTFS，局域网环境、FTP 服务器、PGP 8.1 中文版软件。

13.2　PGP 简介与基本功能

PGP，全称 Pretty Good Privacy，一种在信息安全传输领域首选的加密软件，其技术特性是采用了非对称的“公钥”和“私钥”加密体系。由于美国对信息加密产品有严格的法律约束，特别是对向美国、加拿大之外国家散播该类信息，以及出售、发布该类软件约束更为严格。因此限制了 PGP 的发展和普及，现在该软件的主要使用对象为情报机构、政府机构、信息安全工作者(例如较有水平的安全专家和有一定资历的黑客)，PGP 最初的设计主要是用于邮件加密，如今已经发展到了可以加密整个硬盘、分区、文件、文件夹、集成进邮件软件进行邮件加密，甚至可以对 ICQ 的聊天信息实时加密。用户双方只要安装了 PGP，就可利用其 ICQ 加密组件在用户双方聊天的同时加密或解密，和正常使用没有什么差别，最大程度地保证了网络两端用户的聊天信息不被窃取或监视。

13.2.1　安装

和其他软件一样，运行安装程序后，经过短暂的自解压准备安装的过程后，进入安装界面，先是欢迎信息，单击 NEXT 按钮，然后是许可协议，这是必须无条件接受的。单击 YES 按钮，进入提示安装 PGP 所需要的系统以及软件配置情况的界面，建议阅读一下，继续单

击 NEXT 按钮，出现创建用户类型的界面，如图 13.1 所示。



图 13.1　创建用户类型

选择“No，I’m a New User”，这是告诉安装程序是新用户，需要创建并设置一个新的用户信息。继续单击 NEXT 按钮，来到了程序的安装目录(安装程序会自动检测系统，并生成以系统名为目录名的安装文件夹)建议将 PGP 安装在安装程序默认的目录，也就是系统盘内，程序很小，不会对系统盘有什么大的影响。再次单击 NEXT 按钮，出现选择 PGP 组件的窗口，安装程序会检测系统内所安装的程序，如果存在 PGP 可以支持的程序，它将自动选中该支持组件，如图 13.2 所示。

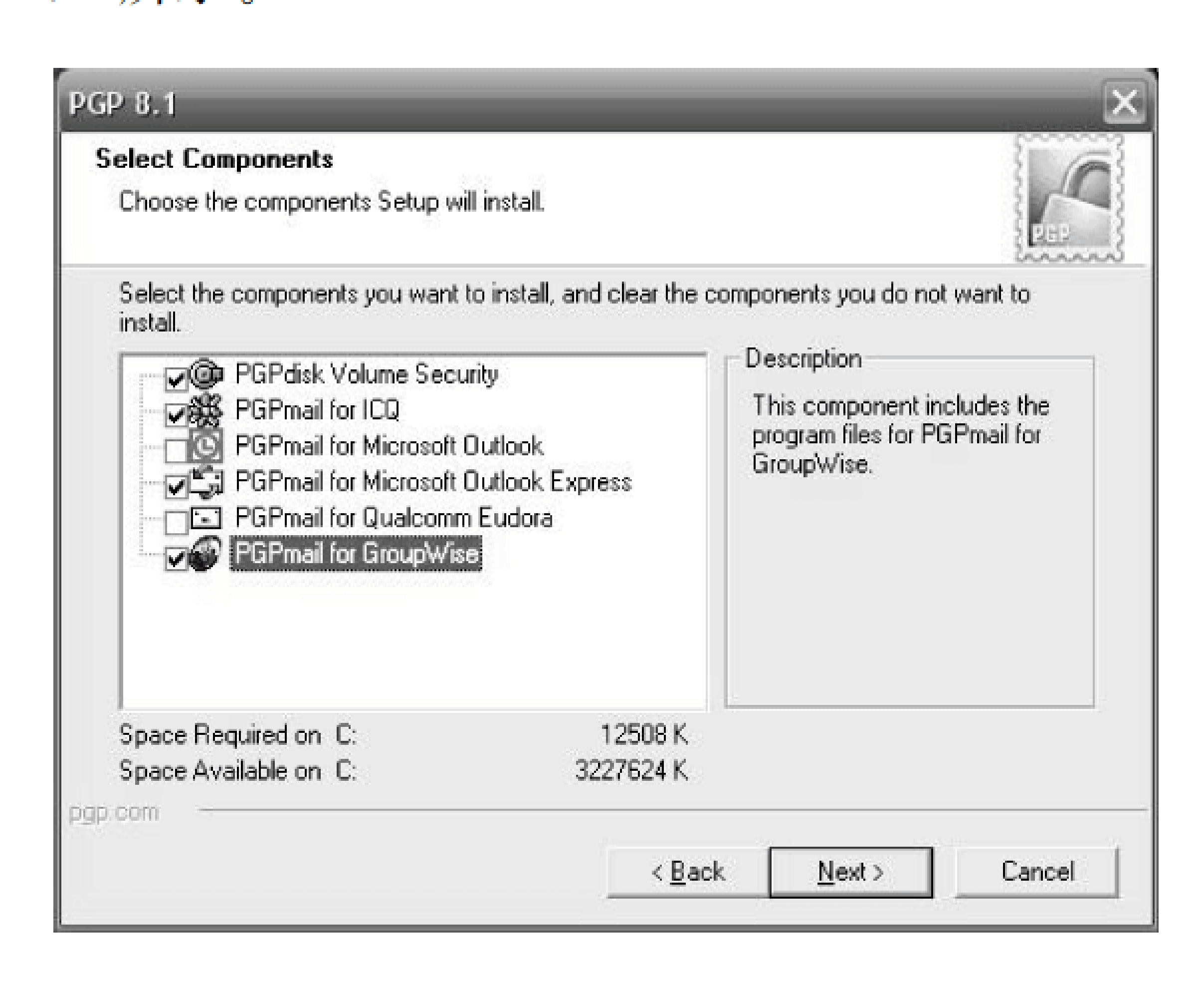


图 13.2　选择组件

第一个是磁盘加密组件，第二个是 ICQ 实时加密组件，第三个是微软的 Outlook 邮件加密组件，第四个是 Outlook Express 加密组件，第五个 Qualcomm Eudora，是一套功能全面的 E-Mail 客户端软件和第六个组件 Groupwise 是 Novell 公司的邮件服务器。后面的安装过程就只需一直单击 NEXT 按钮，最后再根据提示重新启动系统即可完成安装。

13.2.2　创建和设置初始用户

重启后，进入系统时会自动启动 PGPtray. exe，这个程序是用来控制和调用 PGP 的全

部组件的，如果没有必要每次启动的时候都加载它，可以这样取消它的启动：选择“开始”→“所有程序”→“启动”，在这里删除 PGPtray 的快捷方式即可。接下来进入新用户创建与设置。启动 PGPtray 后，会出现一个“PGP 密钥生成向导”，单击“下一步”按钮，进入“用户名和电子邮件分配”界面，在“全名”处输入想要创建的用户名，“Email 地址”处输入用户所对应的电子邮件地址，完成后单击“下一步”按钮，如图 13.3 所示。

PGP 密钥生成向导

分配姓名和电子信箱
每一个密钥对都有一个与其关联的姓名.姓名和电子信箱地址让你的通信人知道他们正在使用的公钥属于你.

全名(F): abc

被关联的电子信箱地址和你的密钥对,你将会使PGP协助你的通信人在与你通信时选择正确的公钥.

Email地址(E): abc@sina.com.cn

< 上一步(B) 下一步(N) > 取消

图 13.3　用户名和电子邮件分配

接下来进入“分配密码”，在“密码”处输入需要的密码，在“确认”处再输入一次，长度必须大于 8 位，建议为 12 位以上，如果出现“Warning：Caps Lock is activated!”的提示信息，说明开启了 Caps Lock 键(大小写锁定键)，按一下该键关闭大小写锁定后再输入密码，因为密码是要分大小写的。最好别取消“隐藏键入”的选择，这样就算有人在后面看着你输入，也不会那么容易就让他知道你的输入到底是什么，更大程度地保护密码安全。完成后单击“下一步”按钮，如图 13.4 所示。

PGP 密钥生成向导

分配密码
你的私钥将会被密码保护.这些信息很重要且是机密的,你不要将它写下来.

你的密码至少应该有 8 位字符长度,并包含数字和字母

☑隐藏键入(H)

密码(P):

密码强度:

确认(C):

< 上一步(B) 下一步(N) > 取消

图 13.4　密码输入和确认

进入密钥生成进程，等待主密钥(Key)和次密钥(Subkey)生成完毕。单击“下一步”按钮，进入“完成该 PGP 密钥生成向导”再单击“完成”按钮，用户就创建并设置好了。

13.2.3　导出并分发你的公钥

启动 PGPkeys，在这里将看到密钥的一些基本信息，如有效性(PGP 系统检查是否符合要求，如符合，则显示为绿色)、信任度、大小、描述、密钥 ID、创建时间、到期时间等(如果没有这么多信息，使用菜单里的“查看”命令，并选中里面的全部选项)，如图 13.5 所示。



图 13.5　密钥基本信息

需要注意的是，这里的用户其实是以一个“密钥对”形式存在的，也就是说其中包含了一个公钥和一个私钥。现在要做的就是要从这个“密钥对”内导出包含的公钥。选中刚才创建的用户，在上面右击，选“导出”，在出现的保存对话框中，确认是只选中了“包含 6.0 公钥”，然后选择一个目录，再单击“保存”按钮，即可导出刚才创建用户的公钥，扩展名为.asc。导出后，就可以将此公钥放在指定的网站上，或者发给需要的用户，告诉对方以后发邮件或者重要文件的时候，通过 PGP 使用此公钥加密后再发送过去，这样做一是能防止邮件被人窃取后阅读而泄露个人隐私或者商业机密，二是能排查病毒邮件，一旦看到没有用 PGP 加密过的文件，或者是无法用私钥解密的文件或邮件，就能更有针对性地执行删除或者杀毒操作。虽然比以前的文件发送方式和邮件阅读方式麻烦一点，但却能更安全地保护隐私或公司的秘密。

13.2.4　导入并设置其他人的公钥

导入公钥：直接单击(根据系统设置不同，单击或者双击)对方发给你的扩展名为 asc 的公钥，将会出现选择公钥的窗口，在这里能看到该公钥的基本属性，如有效性、创建时间、信任度等，便于了解是否应该导入此公钥。选好后，单击“导入”按钮，即可导入进 PGP，如图 13.6 所示。



图 13.6　导入公钥

设置公钥属性：接下来打开 PGPkeys，就能在密钥列表里看到刚才导入的密钥，如图 13.7 所示。



图 13.7　公钥属性

选中它，右击，选“密钥属性”，这里能查看到该密钥的全部信息，如是否是有效的密钥，是否可信任等，如图 13.8 所示。

在这里，如果直接拉动“不信任的”的滑块到“信任的”，将会出现错误信息。正确的做法应该是关闭此对话框，然后在该密钥上右击，选“签名”，在出现的“PGP 密钥签名”对话框中，单击“确定”按钮，会出现要求为该公钥输入密码的对话框，这时输入设置用户时的那个密码，然后继续单击“确定”按钮。即完成签名操作，查看密码列表里该公钥的属性，应该在“有效性”栏显示为绿色，表示该密钥有效。然后再右击，选“密钥属性”，将“不信任的”处的滑块拉到“信任的”，再单击“关闭”按钮即可，这时再看密钥列表里的那个公钥，“信任度”处就不再是灰色了，说明这个公钥被 PGP 加密系统正式接受，可以投入使用了。关闭 PGPkeys 窗口时，可能会出现要求备份的窗口，建议选择“现在备份”按钮选择一个路径保存，比如“我的文档”(此备份的作用是防止下次使用的时候意外删除了重要用户，可以用此备份恢复)。



图 13.8　密钥的全部信息

13.2.5　使用公钥加密文件

不用开启 PGPkeys，直接在你需要加密的文件上右击，会看到一个叫 PGP 的菜单组，进入该菜单组，选“加密”，将出现“PGP 外壳-密钥选择对话框”，如图 13.9 所示。

在这里可以选择一个或者多个公钥，上面的窗口是备选的公钥，下面的窗口中是准备使用的公钥，双击备选窗口中的某个公钥，即对其进行了加密操作，该公钥就会从备选窗口转到准备使用的窗口中，已经在准备使用窗内的，如果不想使用它，也通过双击的方法，使其转到备选窗口。选择好后，单击“确定”按钮，经过 PGP 的短暂处理，会在想要加密的那个文件的同一目录中生成一个格式为：“加密的文件名.pgp”的文件，这个文件就可以用来发送了，注意，刚才使用哪个公钥加密的文件，只能发给该公钥的所有人，别人无法解密。只有该公



图 13.9　密钥选择对话框

钥所有人才有解密的私钥。如果要加密文本文件，如 txt 文件，并且想要将加密后的内容作为论坛的帖子发布，或者要作邮件内容发布，那么，就在刚才选择公钥的窗口中，选中左下脚的“文本输出”，这样创建的加密文件将是这样的格式：“加密的文件名.asc”，用文本编辑器打开的时候看到就不是没有规律的乱码了（不选择此项，输出的加密文件将是乱码），而是很有序的格式，便于复制。将“测试一下”这几个字加密后，显示结果如图 13.10 所示。



图 13.10　加密后的密文

PGP 还支持创建自解密文档，只需要在刚才选择公钥的对话框中选中“自解密文档”再单击“确定”按钮，输入一个密码，单击“确认”按钮，再确认一次，出现保存对话框，选一个位置保存即可。这时创建的就是：“加密的文件名.sda.exe”这样的文件，这个功能支持文件夹加密，类似 WINZIP 以及 WINRAR 的压缩打包功能。说到这里，值得一提的是，PGP 给文件进行超强的加密之后，还能对其进行压缩，压缩率比 WINRAR 小不了多少。很利于网络传输。

13.2.6　文件、邮件解密

使用 PGPtray 解密：文本形式的 PGP 加密文件，可以使用 PGPtray 的两种方式解密。先用文本编辑器打开，会看到类似图 13.10 里的字符，在右下脚找到 PGPtray 图标（锁的形

状)，在上面右击，选择“当前窗口”→“解密和效验”，如图 13.11 所示。



图 13.11　解密和效验

根据提示输入密码，单击 OK 按钮，就会弹出文本查看器，显示出加密文本的明文内容，成功完成解密。还可通过复制加密文本的内容，然后在 PGPtray 图标上右击，选择“剪贴板”→“解密和效验”，也可以完成解密。使用 PGPshell 解密：文本类型的加密文件可将内容复制后保存为一个独立的文件，比如解密.txt，然后在文件上右击，选择 PGP 菜单组内的“加密”，将弹出对话框，要求输入密码，输入正确的密码后，弹出保存解密后文件的对话框，选择一个路径保存即可。其他类型的加密文件，重复上面的 PGP 菜单组内的“加密”操作即可完成解密。

13.3　PGPmail 的使用

13.3.1　PGPmail 简介

PGPmail 是用来加密保护邮件信息和文件中的隐私，唯有接收者通过他们的私钥才能读取。还可以对信息和文件进行数字签名，使之保证其可靠性。签名可证实信息没有被任何方式的篡改。

PGP 是由公钥发展而来的，是一个基于 RSA 公钥加密体系的邮件加密软件，它可以用来对邮件加密以防止非授权者阅读，还能对邮件加上数字签名而使收信人可以确信邮件是谁发来的。它让使用者可以安全地和从未见过的人通信，事先并不需要任何保密的渠道用来传递密钥。它采用了审慎的密钥管理，一种 RSA 和传统加密的杂合算法，用于数字签名的邮件文摘算法，加密前压缩等，还有一个良好的人机工程设计。它的功能强大有很快的速度，并且它的源代码是公开的。现在 Internet 上使用 PGP 来进行数字签名和加密邮件非常流行。

使用 PGPmail 来保护 Email，从 PGP 程序组打开 PGPmail，如图 13.12 所示。



图 13.12　PGPmail 界面

图 13.12 所示功能依次如下：

PGPkeys、加密、签名、加密并签名、解密效验、擦除、自由空间擦除。关于上述功能，我将在下面的 PGPmail for Outlook 的组件中进行实验。

下面简述一下 PGPmail 在 OE(Outlook Express)中的使用。或许是 OE 不太经常使用的缘故，PGPmail 对 OE 附加的功能不是太完美，就比如说不支持在 OE 邮件中加密 HTML，当然可以作为附件的形式加密。

13.3.2　分发 PGP 公钥并发送 PGP 加密邮件

在使用 PGP 加密通信之前，首先得把自己的公钥分发给需要的人，这样，在他们给你发送加密邮件的时候使用公钥进行加密，然后才能用私钥进行解密读取。

如图 13.13 所示，打开 PGPkeys，在创建的密钥对上右击，选择“发送到”→“邮件接收

人”寄给对方 PGP 公钥。



图 13.13 选择密钥并发送加密邮件

如果系统默认是采用 Outlook 来收发邮件的话，将会开启 Outlook 并附加了公钥，如图 13.14 所示。



图 13.14 开启 Outlook 并附加公钥

填入对方的邮件地址，对方在收到此公钥后就能和你进行 PGP 加密通信了。同样在你收到对方 PGP 公钥的时候，把附件(PGP Public key).asc 导入到 PGPkey 里面。

在 OE 中，如果安装了 PGPmail for OutLook Express 的插件，就可以看到 PGPmail 加载到了 OE 的工具栏里，见图 13.15(带有钥匙的按钮)。

OE 创建新邮件时，检查工具栏“加密信息(PGP)”和“签名信息(PGP)”按钮状态是否按下，如图 13.16 所示。

当书写完纯文本的加密邮件时，填入对方 E-mail 地址。确认后发送，这时 PGPmail 将会对其使用主密钥和对方公钥进行加密，加密后的邮件也只能由通信双方才能使用自己的私钥进行解密。PGPkey 会在服务器上查找相应的公钥，避免对方更新密钥而造成无法收取邮件信息，如图 13.17 所示。



图 13.15　Outlook 收件箱



图 13.16　检查加密信息和签名信息

单击“取消”按钮，弹出 Recipient Selection 接收者选择窗口，从上方的列表中选择相应的接收者，用鼠标双击后添加到下面的接收者列表里，如图 13.18 所示。



图 13.17　连接服务器



图 13.18　添加接收人

设置好之后，单击“确认”按钮，就可以发送通过 PGP 加密的邮件。

可能很多时候会以附件形式寄出邮件，这个时候，打开 PGPmail，在 PGPmail 窗口中，按下“加密”，如图 13.19 所示。

然后选择需要加密的文件，如图 13.20 所示。



图 13.19　PGPmail 界面中按下加密



图 13.20　选择加密文件

确定后在弹出的“PGPmail-密码选择对话框”中，选择所需要使用的公钥进行加密。在图 13.21 中可以看到以下选项。



图 13.21　密码选择对话框

• 文本输出：解密后以文本形式输出。
• 输入文本：选择此项，解密时将以另存为文本输入方式进行加密。
• 粉碎原件：加密后粉碎掉原来的文件，不可恢复。
• 安全查看器：只有用户的眼睛才能查看。其实是使用了 TEMPEST 防攻击字体进行模糊化，其实是为了防止监视设备监视用户的显示器，应用到很多军方、政府领域。
• 常规加密：输入密码后进行常规加密，有点局限性。
• 自解密文档：继承于“常规加密”，此方式也经常使用到，通常加密目录下的所有文件。

这里以“文本输出”为例，选中后，拖曳(或双击)对方的公钥到接收人列表里，确定后，文

件将以此公钥来进行加密，对方使用密钥才能进行解密。加密后的文件“*.asc”如图13.22所示。





图13.22　加密前后的文件图标

在邮件中加入此附件寄出就可以了。

如果选择“安全查看器”，将会弹出一个警告窗口，以此来确认使用“安全查看器”，如图13.23所示。

否则的话取消即可，解密时输入密码显示如图13.24所示。

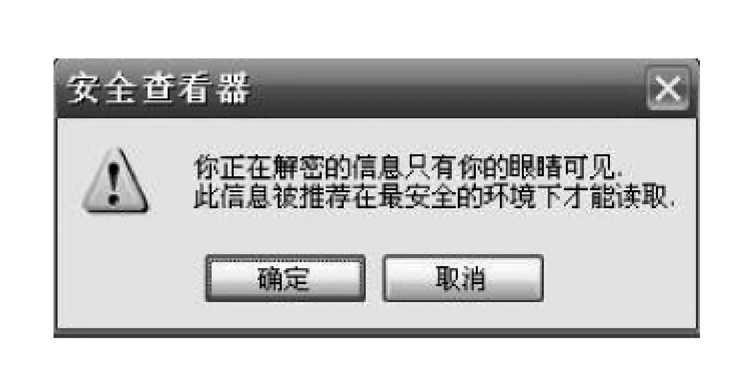


图13.23　安全查看器警告窗口

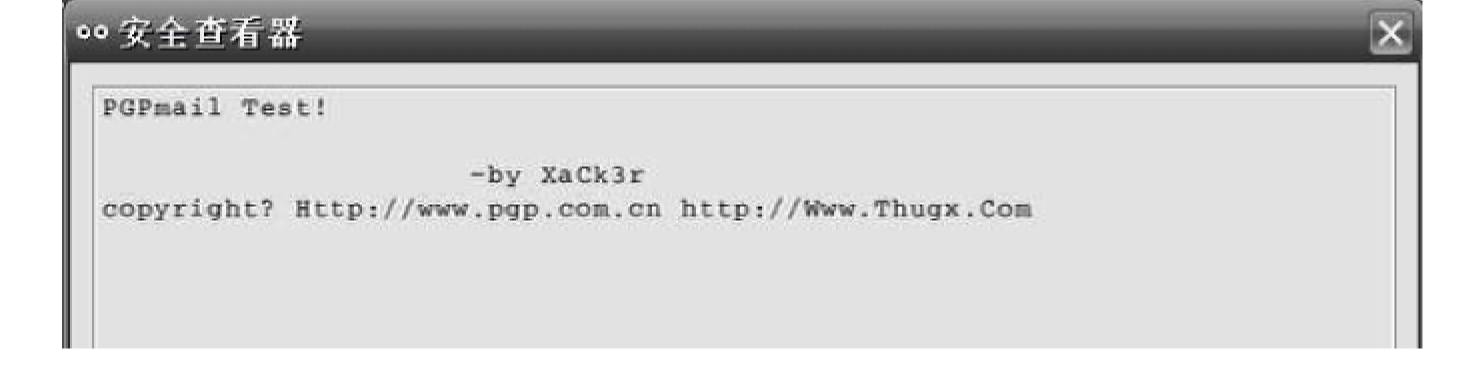


图13.24　安全查看器内容

13.3.3　收取PGP加密邮件

连接服务器并使用Outlook收取PGP加密邮件，打开时，如图13.25所示。



图13.25　Outlook收取PGP加密邮件

看到的是乱码(PGP加密后的信息)，这时，在任务栏单击PGP图标，在弹出的菜单中选择“当前窗口”→“解密 & 效验”，如图13.26所示。

在弹出如图13.27所示的窗口中输入设定的密钥密码。

成功后将会解密邮件信息，并弹出文本查看器窗口，这个时候已经看到解密后的信息

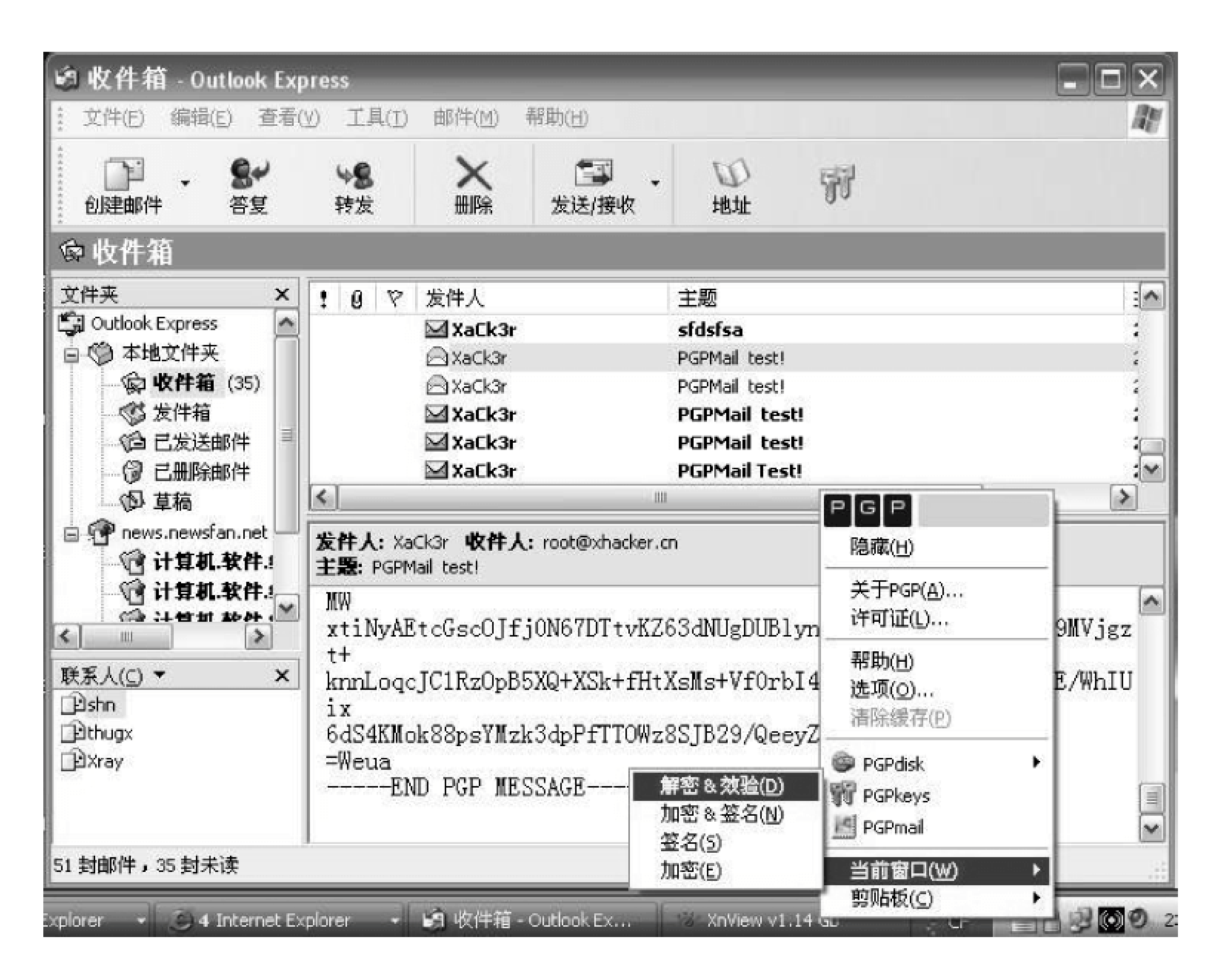


图 13.26 解密 & 效验



图 13.27 输入密码

了，如图 13.28 所示。

如果含有加密附件时，下载回来在本地打开，如图 13.29 所示，输入相应的密码，即可对文件进行解密并保存。

安全擦除文件，有的时候一些重要的数据，用户不希望留在系统里面，简单的删除不能达到所希望的效果，为了防止被非授权的用户通过恢复来查看数据，可以采用 PGPmail 来安全擦除数据，进行多次反复写入，那样就可以达到无法恢复的效果。并且还可以对整个磁盘分区进行覆写。

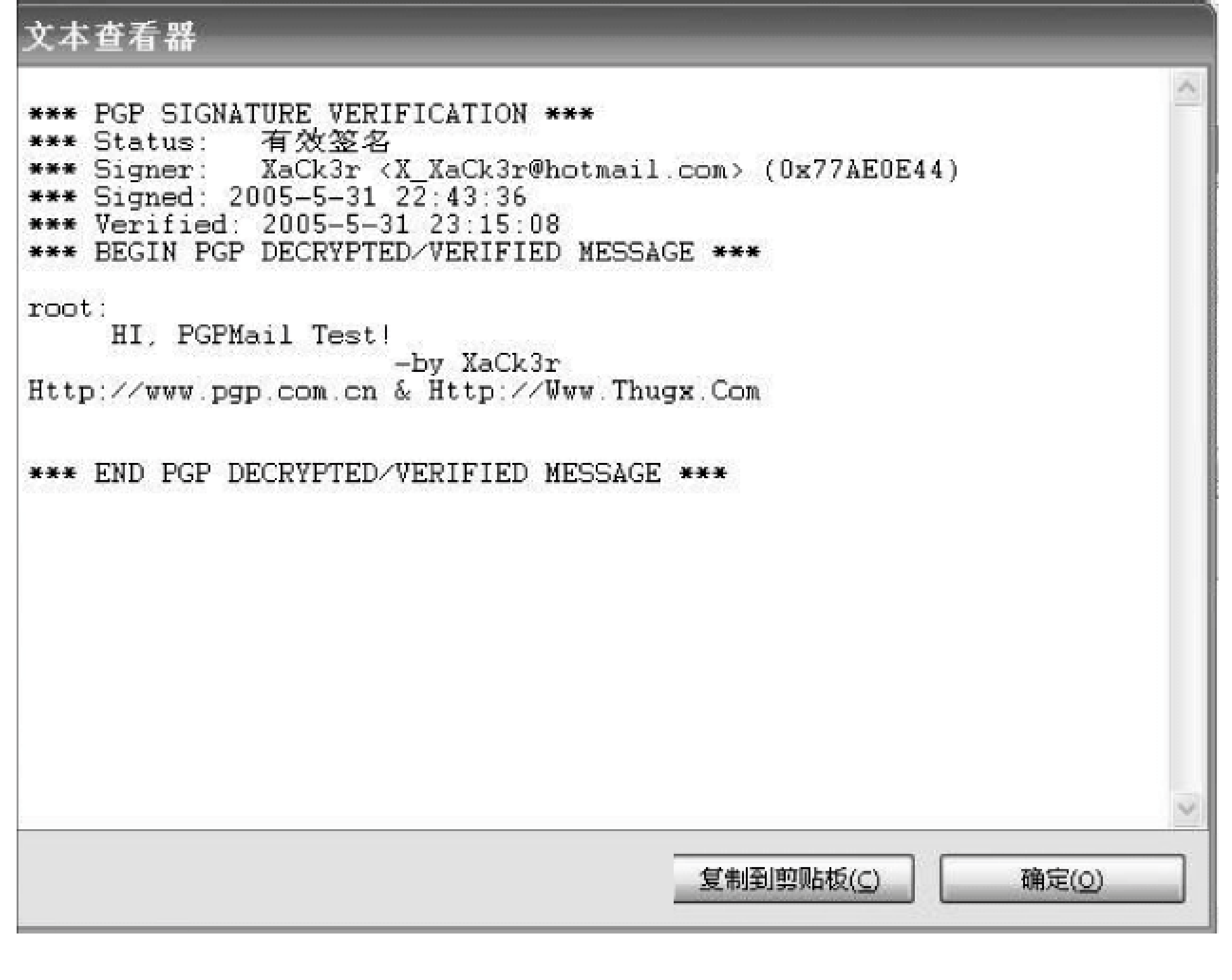




图 13.28　文本查看器窗口



图 13.29　对文件进行解密并保存

13.3.4　创建自解密文档

这个功能经常被用到,在很多情况下,用户收到了加密数据,但计算机中没有安装 PGP 软件,这个功能就起到了作用,创建自解密后的文件可以脱离 PGP 环境运行。在 PGP 环境下,在你所需要加密的文件上右击,在弹出的 PGP 组中选择"创建 SDA(C)",如图 13.30 所示。

然后在弹出的窗口中输入密码,如图 13.31 所示。



图 13.30　创建 SDA



图 13.31　输入密码

确定后弹出选择保存文件的对话框,如图 13.32 所示。

单击"保存"按钮即可,所在目录下就会生成一个.exe 后缀的文件,如"创建 SDA.txt.sda.exe",双击打开,如图 13.33 所示。

在图 13.33 所示界面下输入正确密码就可以进行解密了。以后可以采用此加密方式来取代 WINRAR 压缩软件进行打包,而且它的压缩率也很高。




图 13.32　保存文件



图 13.33　创建自解压文件

13.4　PGPdisk 的使用

13.4.1　PGPdisk 简介

PGPdisk 是一个使用方便的组件，能够划分出一部分磁盘空间来存储敏感数据。这个专用的空间用于创建一个叫做 PGPdisk 的卷。虽然它是一个单独的文件，一个 PGPdisk 卷却非常像一个硬盘分区，来提供存储文件和应用程序。可以认为它是一个软盘或者一个外置的硬盘。以下把使用 PGPdisk 卷称之为装配。

当一个 PGPdisk 卷被装配上去的时候，可以用它作为其他不同的盘。可以安装程序在此卷下或者移动、保存文件到卷里。当卷被反装配时，如果不知道密码，将无法访问它，它能使整个卷受到保护。它存储着加密的格式，除非一个文件或者程序正在使用。如果计算机遇到崩溃的情况，此卷的内容依然是加密着的。

很多时候，如果硬盘里存储着一些敏感的数据，而且不太经常使用，那就可以创建一个 PGPdisk 卷来加密这些硬盘数据，需要时再装配它。

13.4.2　创建 PGPdisk

首先在任务栏右下角单击 PGPdisk 的图标或者在开始菜单 PGP 程序组里面选择 PGPdisk 打开“PGPdisk 创建向导”界面，如图 13.34 所示。

出现如图 13.35 所示的界面，这里概括出了 PGPdisk 的基本功能。

单击“下一步”按钮，如图 13.36 所示。指定要存储这个“ *.pgd”文件的位置和容量大小。这个“.pgd”文件将在以后被装配为一个卷，也可以理解为一个分区，可以随时装配使用。

这里选择“高级选项”进行配置，如图 13.37 所示。

可以让它以一个分区形式存在，或者在 NTFS 分区上作为一个目录，这里作为一个目录；然后就是选择算法，三种密码算法可供选择：AES(256 bits)、CAST5(128bits)、



图 13.34　开始创建向导



图 13.35　PGPdisk 介绍



图 13.36　指定.pgd 文件的位置和容量



图 13.37　高级选项

Twofish(256 bits)。接下来选择文件系统格式,可作为 FAT 或者 NTFS 装配使用。可以根据需要选择"启动时装配"。确定后返回到上一个界面。单击"下一步"按钮,确定保护方法,如图 13.38 所示。



图 13.38　选择保护方式

在这里可以使用全面已经建好的密钥对，推荐就用自己的公钥来进行加密保护，这里使用已建立的公钥对其进行加密保护，选择“公钥”，单击“下一步”按钮，如图 13.39 所示。



图 13.39　选择公钥

如果已经建立过自己的密钥，列表中将会出现所建立的密钥信息，选中双击或者单击“下一步”按钮，如图 13.40 所示。

这个进度条显示了 PGPdisk 卷将被初始化和格式化，并且通过鼠标移动来进行随机加密，单击“下一步”按钮，PGPdisk 为用户所指定的卷进行加密和格式化操作，这里可能会需要花点时间，根据卷的大小而定，如图 13.41 所示。



图 13.40　收集随机数据

这里基本上已经完成了 PGPdisk 的创建，单击“下一步”按钮，如图 13.42 所示。

完成安装，成功后如图 13.42 所示，给出了一些相关反装配的信息，下面进行装配使用。

13.4.3　装配使用 PGPdisk

前面已经创建了 PGPdisk 卷，选择“我的计算机”→“D：盘”，将会看到已经装配了一个新的文件夹(PGPdisk)，以后机密数据都可以存储在该文件夹下，不使用的时候，选择反装配，可以在卷上右击选择反装配，或者从 PGP 程序组里的 PGPdisk 中选择“反装配所有磁

盘”进行反装配，如图 13.43 所示。



图 13.41　PGPdisk 卷初始化和格式化



图 13.42　完成安装



图 13.43　反装配所有磁盘

PGPdisk 对用户组提供了强有力的支持，如果一些硬盘分区或者移动存储设备需要提供给别人使用而又不希望任何人可轻易使用，这就可以针对个别用户进行权限分配。下面介绍 PGPdisk 的强大功能。

在图 13.43 中出现的菜单中选择“编辑 PGPdisk(E)”，或者在创建的“*.pgd”文件上右击，在出现的菜单中选择 PGP→“编辑 PGPdisk(E)”，也可从 PGPdisk 中选择“编辑磁盘(E)”，进入图 13.44 所示界面。注意在添加用户的时候，必须进行反装配。

在图 13.44 中单击“添加”按钮，这个时候将会弹出一个密码提示框，输入密钥的正确密码进入“PGPdisk 用户创建向导”，如图 13.45 所示。

单击“下一步”按钮，采用对方公钥或者密码来进行保护，但不同的是，可以指定用户的读写权限。这里选择公钥来加密保护。继续单击“下一步”按钮，出现所有 PGPkeys，如图 13.46 所示。

选择允许访问的用户，也可以通过 Ctrl 键多选，单击“下一步”按钮，再单击“完成”按钮后，回到 PGPdisk 管理界面。在这里，可以管理用户组，对用户进行“移除”、“禁用”、“固定

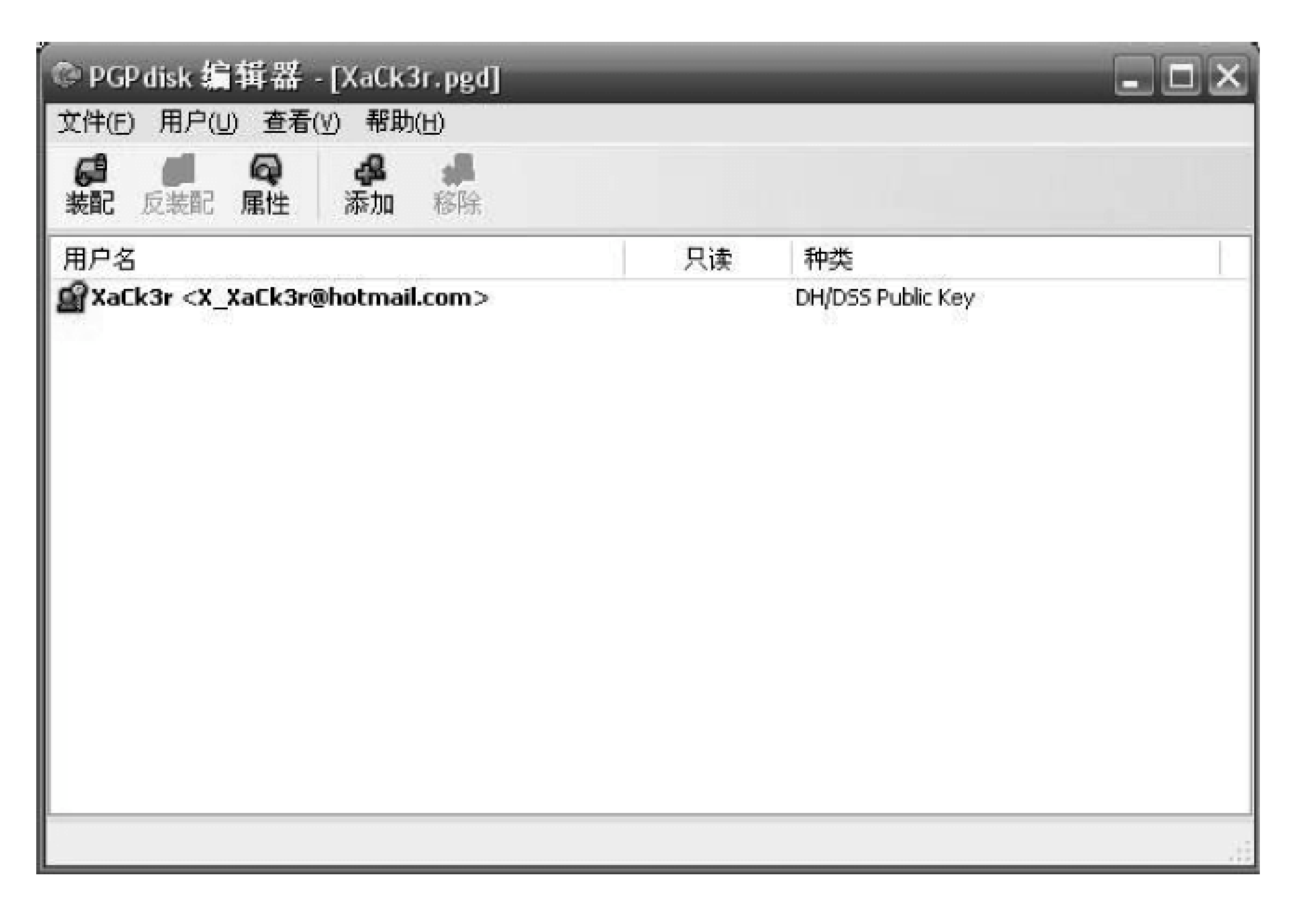


图 13.44 编辑 PGPdisk



图 13.45 PGPdisk 用户创建向导



图 13.46 选择公钥

为只读"等操作,如图 13.47 所示。



图 13.47 管理用户组

还可以设置一个管理员来对其进行管理,前提是在添加一个新用户的时候,选择加密保护方式为密码保护。

13.4.4 PGP 选项

1. 常规

如图 13.48 所示,分别有几个选项,"总是用默认的密钥加密",该选项可根据实际需要选择,如果经常给其他用户传输文件,需要用其他用户的公钥进行加密,建议不要选择此项。



图 13.48 PGP 选项

选中"更快地生成密钥",可减少创建密钥所花的时间。

在"第一登录"选项组内的选项可根据自己的情况而设定,有的时候,频繁地使用密钥来进行加密、解密、验证、签名等之类的,如果每次都这样重复输入显得很麻烦,这个时候就可

以使用密码缓存功能,这样短时间内就不需要重复地输入密码了。

“文件粉碎”主要针对的是一些反删除软件,在日常运用中的删除,其实是简单意义上的删除,数据还是存在的,一些反删除软件就可以对其进行恢复,所以 PGP 里提供的“文件粉碎”是个很不错的功能选择,它对文件所在的硬盘的地方进行反复写入数据,让一些反删除软件无能为力。

2. 文件

如图 13.49 所示,这里是密钥环的位置,主要注意的是备份好密钥环文件,手动或者自动都可以。PGP 默认在系统盘的 My Document 下建议更改文件夹,以防止系统崩溃未能作到及时备份。这里有个技巧,很多软件都会往“我的文档”写入一些数据,如果把“我的文档”定向到其他分区就免去了每次转移的麻烦。

3. 邮件

如图 13.50 所示,“默认签名新消息”,这样可以在对方装有 PGP 的环境下验证邮件的有效性,确认是否是你发出,或者在传输过程中被第三方篡改。



图 13.49　密钥环文件



图 13.50　邮件的设置

选择“打开信息时自动解密/效验”会将更快更方便地解密/效验邮件。

4. 高级

如图 13.51 所示的选项很容易明白,加密算法支持,该注意的地方是前面提到的备份,在这里,选“在 PGPkeys 关闭时自动密钥对备份.(B)”选项,可以另外选择一个文件夹来做备份,如图中的“X:\”,用于有额外的硬盘空间。

另外补充一点,不要选中“自动检查软件更新”否则会总是提示升级到 9.0。毕竟现在 PGP9.0 还非正式版本,会出现不稳定的情况,而 PGP 8.1 可作为长期免费使用。

5. PGPdisk

如图 13.52 所示,“允许强制反装配 PGPdisk 打开的文件夹(F)”,某些情况下,在 PGPdisk 卷中有打开的文件,PGPdisk 就无法反装配它,选中此项,PGPdisk 将强制反装配 PGPdisk 卷即使在 PGPdisk 卷中有打开的文件。



图 13.51　高级选项



图 13.52　PGPdisk 选项

"自动反装配",建议选中此项,并设定时间,在未使用的时候,自动进行反装配,但在这里,如果 PGPdisk 卷中有打开的文件,就不能进行反装配。

实验思考题

1. 如何保证密钥能够安全地发布和交换?
2. 比较用 PGP 创建自解密文档与 WINRAR 创建的压缩文件哪个压缩比例高?
3. PGPdisk 的功能和 Windows 自带的文件加密系统的比较与区别?

第14章 实验5 防火墙的安装与使用

14.1 实验目的及要求

14.1.1 实验目的

通过实验掌握防火墙的安装过程、登录防火墙 Web 界面的方式、身份认证的方式、管理员配置的主要内容、常用控制功能的实现等。

14.1.2 实验要求

根据本教材中介绍的操作步骤完成实验内容,详细观察操作结果并记录设置的内容,理解设置的内容和原理,做出分析并写出实验总结报告。

14.1.3 实验设备及软件

3 台安装 Windows 2000/XP 操作系统的计算机,1 台锐捷防火墙、相关证书、私钥等。

14.2 登录防火墙 Web 界面

14.2.1 管理员证书

管理员可以用证书方式进行身份认证。证书包括 CA 证书、防火墙证书、防火墙私钥、管理员证书。前三项必须导入防火墙中,后一个同时要导入管理主机的 IE 中。

证书文件有两种编码格式:PEM 和 DER,后缀名可以有 pem、der、cer、crt 等多种,后缀名与编码格式没有必然联系。

CA 证书、防火墙证书和防火墙私钥只支持 PEM 编码格式,cacert.crt 和 cacert.pem 是完全相同的文件。管理员证书支持 PEM 和 DER 两种,因此提供 administrator.crt 和 administrator.der 证书,administrator.crt 和 administrator.pem 是完全相同的文件。*.p12 文件是将 CA、证书和私钥打包的文件。

导入证书:

选择 IE 浏览器的"工具"→"Internet 选项"→"内容"→"证书",操作过程如图 14.1 至图 14.5 所示。

在"证书"对话框中选择"导入"按钮,如图 14.2 所示。

在硬盘上找到证书所在目录,双击打开"admin.p12"文件,如图 14.3 所示。



图 14.1　选择证书选项



图 14.2　导入证书

在对话框中输入默认密码(123456)后,单击“下一步”按钮,如图 14.4 所示。



图 14.3　选择证书

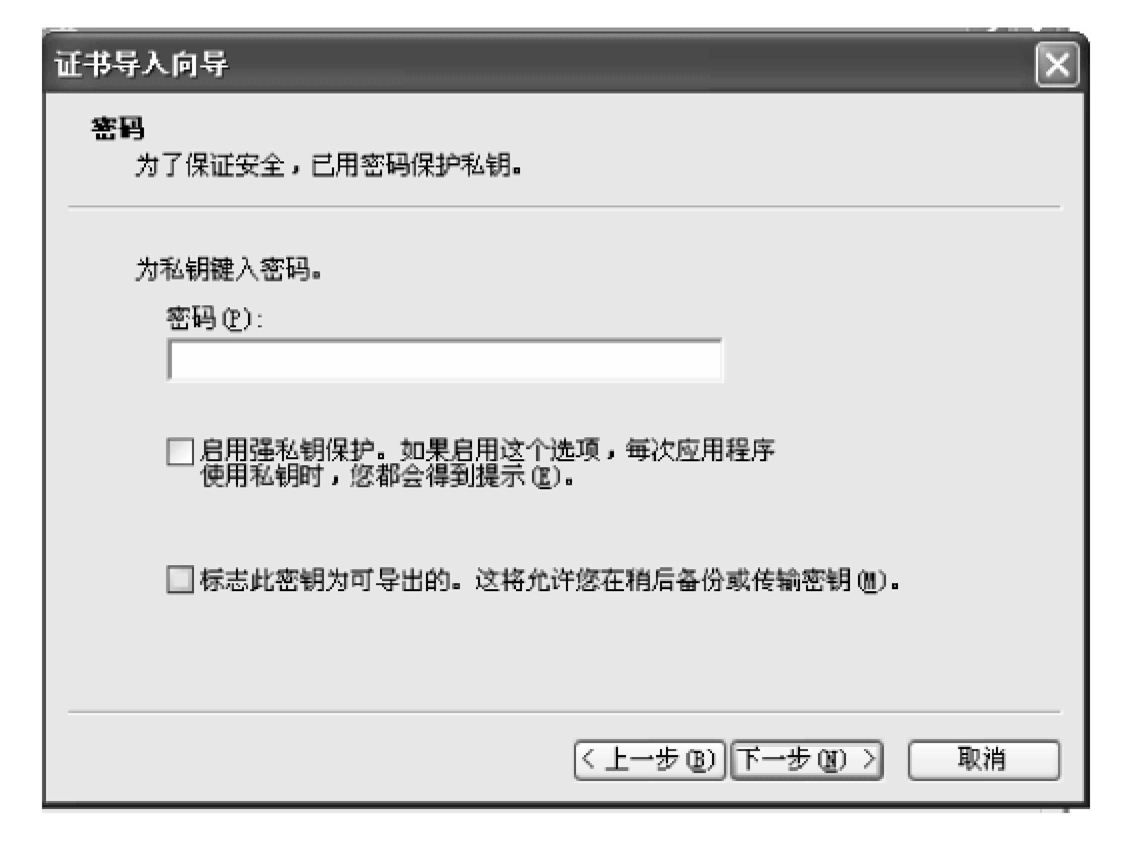


图 14.4　密码为 123456

导入成功后会出现如图 14.5 所示。



图 14.5　导入成功后的状态

14.2.2 管理员配置管理

在管理主机上,通过电子钥匙认证或管理员证书认证成功后,才能访问防火墙,完成对防火墙的配置管理。

防火墙管理 IP 地址:管理员要在防火墙上定义防火墙可以被管理的 IP 地址,并指定管理主机可以进行的操作(如允许 PING、允许 TRACEROUTE 等)。未指定为管理 IP 的主机不能管理。

管理主机地址限制:只有管理主机才能对防火墙进行管理。防火墙系统指定管理主机的 IP,最多可以指定 256 个管理主机,不包括集中管理主机。

管理员身份认证方式:电子钥匙认证和证书认证。

管理员授权:管理员有不同的身份,分为超级管理员、配置管理员、审计管理员、策略管理员。其中,超级管理员可以增加、删除管理员账号;配置管理员可以设置系统配置、管理配置、网络配置;策略管理员可以配置对象定义、安全策略;审计管理员可以查看防火墙日志信息。

管理员访问信道加密:为防止管理员与防火墙之间的管理信息被非法者截取而利用,对防火墙的远程管理的通信应该实现加密。同时,防火墙可以防止对远程管理的重放攻击。CLI 界面命令行方式下支持 SSH 加密,Web 界面下支持 SSL 加密(使用 https 协议访问防火墙)。通过防火墙本地串口使用超级终端登录时通信不加密。

14.2.3 管理员首次登录

正确管理防火墙前,需要配置防火墙的管理主机、管理员账号和权限、网口上可管理 IP、防火墙管理方式。

默认管理员账号为 admin、密码为 firewall、默认管理口:防火墙 WAN 口。

可管理 IP:WAN 口上的默认 IP 地址为 192.168.10.100/255.255.255.0。

管理主机:默认为 192.168.10.200/255.255.255.0。

默认管理方式共有三类:

(1) 管理主机用交叉线与 WAN 口连接。

(2) 用电子钥匙进行身份认证。

(3) 访问 https://192.168.10.100:6667(注:若用证书进行认证,则访问 https://192.168.10.100:6666)。

登录账号为默认管理员账号与密码,访问 Web 界面。此方式下的配置通信是加密的。

14.2.4 登录 Web 界面

将默认管理主机的网口用交叉连接的以太网线(两端线序不同)与防火墙的 WAN 口连接,管理主机的 IE 版本必须是 5.5 及以上版本,如果管理主机是采用电子钥匙认证,需要将与防火墙匹配的电子钥匙插入管理主机上(USB 口),正确输入电子钥匙 PIN 码(初始 PIN 码为:12345678)后,打开防火墙管理员身份认证程序。如果出现绿色图标表示认证通过,出现红色图标表示认证失败或未登录。认证成功后在浏览器中输入

https://192.168.10.100:6667，如果管理主机是采用证书认证，选择要使用的数字证书，如图 14.6 所示，然后输入 https://192.168.10.100:6666。

登录成功后弹出下面的登录界面，如图 14.7 所示。



图 14.6　证书认证



图 14.7　登录界面

正确输入默认管理员账号与密码，进入下面的防火墙配置管理界面，如图 14.8 所示。

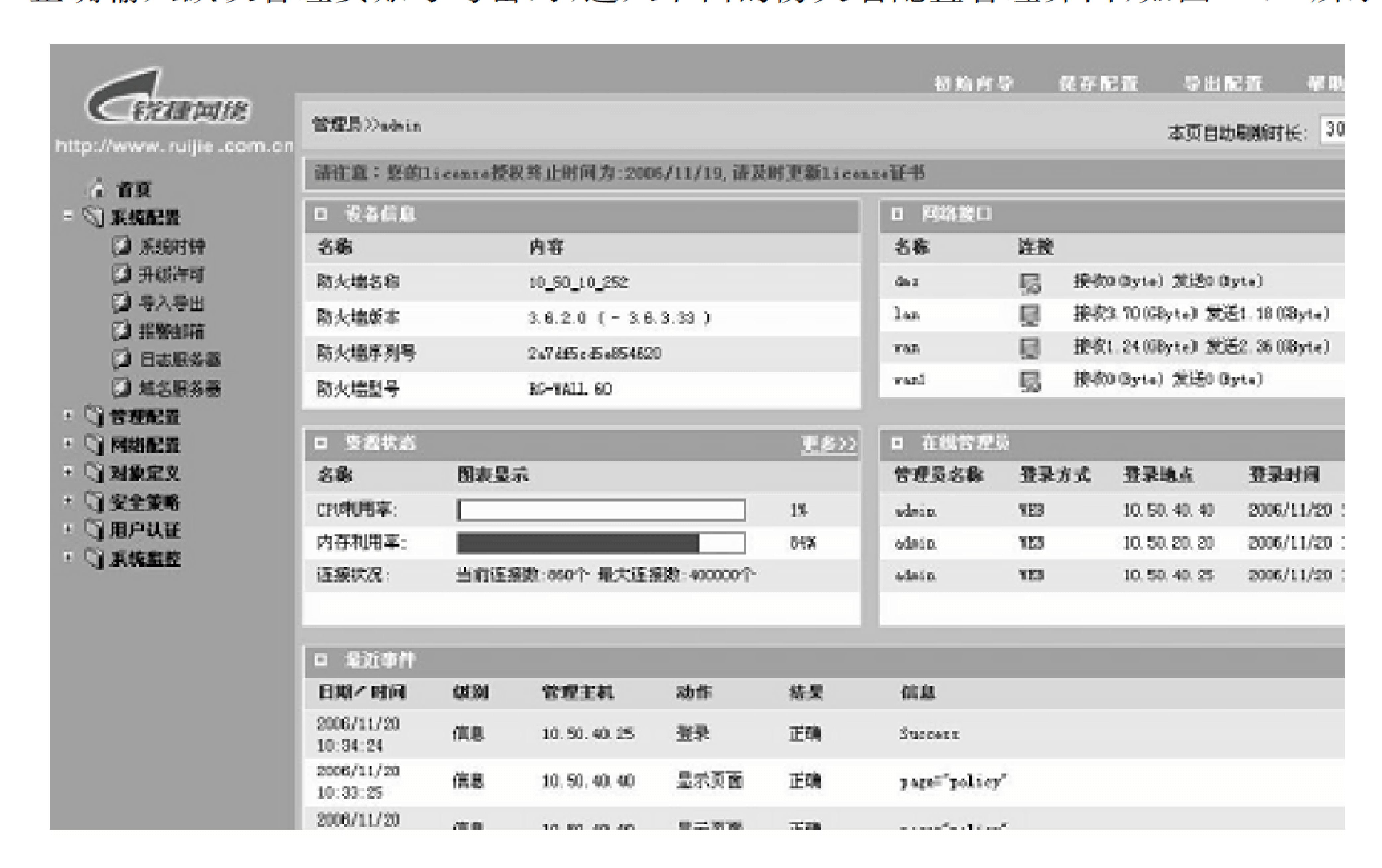


图 14.8　防火墙配置管理界面

在第一次登录成功后，管理员可以按需求变更管理员账号、管理主机、防火墙可管理 IP、管理方式或导入管理员证书。下次登录时，按变更内容进行认证与登录。

当管理员完成管理任务或者离开管理界面时，应主动退出 Web 管理界面。正确的操作方法是单击快捷菜单最右端的“退出”快捷图标，这将通知防火墙本管理员退出操作，然后关闭本窗口。如果单击 IE 标题栏上关闭按钮的话，则只是关闭了窗口，并没有通知防火墙该管理员已退出管理。防火墙 Web 界面有超时机制，默认超时时间为 600 秒，如果防火墙持续（>600 秒）未接收到 Web 界面操作请求，则超时退出。

当管理员再次登录时，要使管理主机与防火墙的某个网口连接，并为其配置可管理 IP，同时管理员需要电子钥匙进行身份认证或者管理员证书方式认证。

管理员将与防火墙匹配的电子钥匙插入管理主机上，正确输入电子钥匙 PIN 码(初始 PIN 码为：12345678)后，打开防火墙管理员身份认证程序。绿图标表示认证通过，红图标表示认证失败或未登录。认证成功后可以访问 https://防火墙可管理 IP:6667，在登录界面中输入管理员账号与密码，进行防火墙配置管理界面。

使用管理员证书方式时，需要在防火墙上导入管理员证书，在管理主机上导入管理员证书，访问 https://防火墙可管理 IP:6666，认证成功后，进入防火墙配置管理界面。

14.3 防火墙实现带宽控制

14.3.1 背景描述

某学院老师发现，他们学院新开通的 100Mb/s 线路仍然经常性地无法打开网页，经查实学院的学生利用 BT、FlashGet 等软件多线程下载，抢占可用带宽，造成其他人的访问不正常。老师要求必须在防火墙上解决该问题，让单个计算机可用带宽减少。

14.3.2 实验拓扑

实验的拓扑结构如图 14.9 所示。

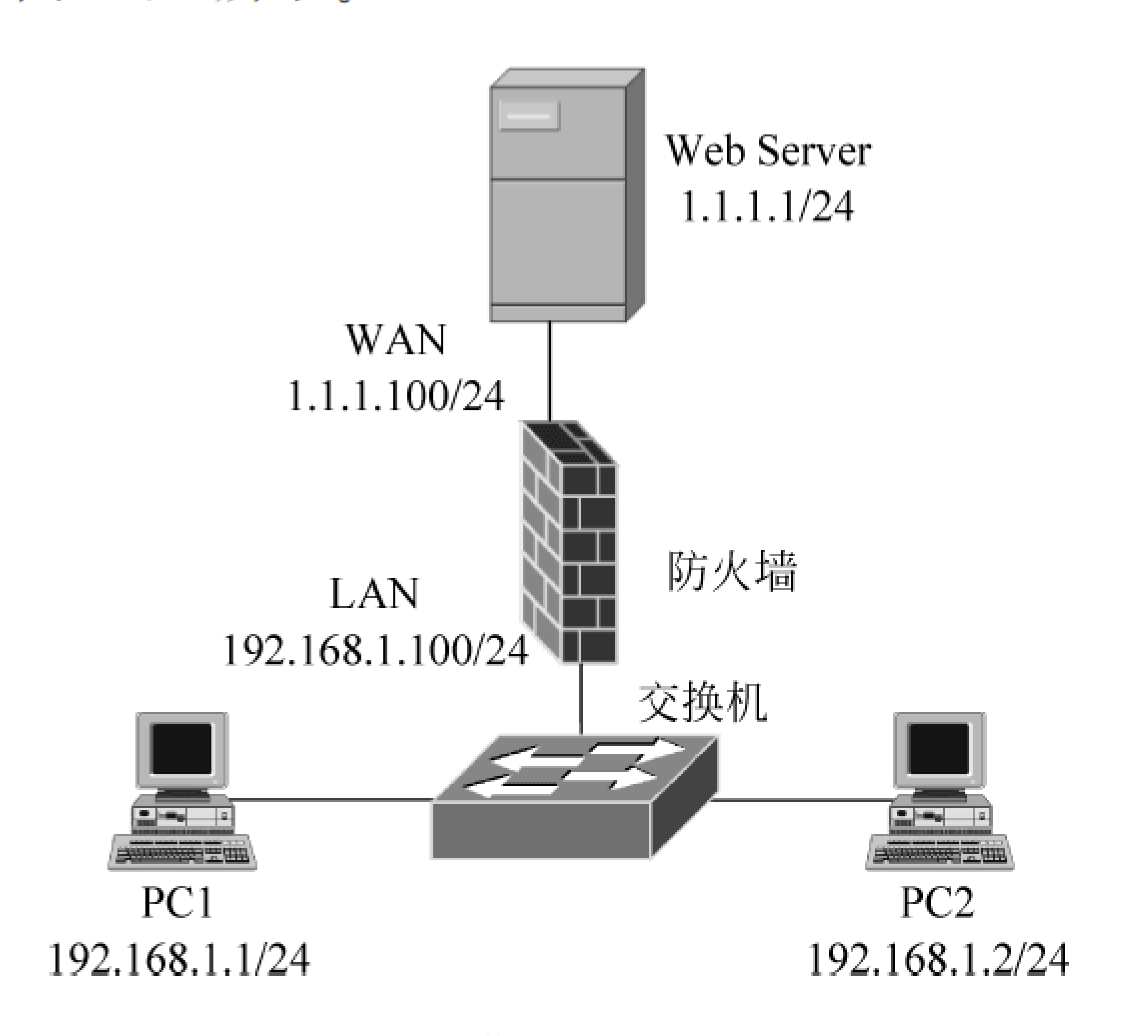


图 14.9　带宽控制实验拓扑

14.3.3 实验原理

利用防火墙中带宽控制功能，将客户机对服务器的访问带宽控制在一定范围内，以达到既可以保证网站被正常访问，也可以作限制，限制每个 IP 可以使用一定数值的带宽。

14.3.4 实验步骤

(1) 按照拓扑正确配置防火墙接口和 PC 的 IP 地址，具体如表 14.1 所示。

表 14.1 IP 规划表

设备名称	IP 地址	子网掩码	默认网关
PC1	192.168.1.1	255.255.255.0	192.168.1.100
PC2	192.168.1.2	255.255.255.0	192.168.1.100
Web Server	1.1.1.1	255.255.255.0	1.1.1.100
防火墙 LAN	192.168.1.100	255.255.255.0	192.168.1.100
防火墙 WAN	1.1.1.100	255.255.255.0	1.1.1.100

(2) 进入防火墙 Web 页面,选择"对象定义"→"带宽列表",创建带宽规则,如图 14.10 所示。



图 14.10 创建带宽规则

(3) 进入防火墙 Web 页面,选择"安全策略"→"安全规则",为 PC1 创建新的包过滤规则,在"流量控制"中选择之前定义的带宽规则 limit,如图 14.11 所示。



图 14.11 创建包过滤规则

(4) 进入防火墙 Web 页面,选择"安全策略"→"安全规则",为 PC2 创建新的包过滤规则,不限制带宽,如图 14.12 所示。



图 14.12 包过滤规则

14.3.5 验证测试

(1) 在 1.1.1.1 服务器上架设 Web 服务器，在 192.168.1.1 上用 IE 下载大文件，计算可下载带宽，最大只能达到 320kb/s。

(2) 在 192.168.1.2 上用 IE 下载大文件，计算可下载带宽，最大带宽大于 320kb/s。

14.4 防火墙实现地址绑定

14.4.1 背景描述

某学院老师发现，他们学院的某些学生经常盗用其他同学的 IP 地址，造成他人不能正常访问网络资源。老师要求必须在防火墙上解决该问题，避免盗用地址的情况出现。

14.4.2 实验拓扑

实验的拓扑结构如图 14.13 所示。

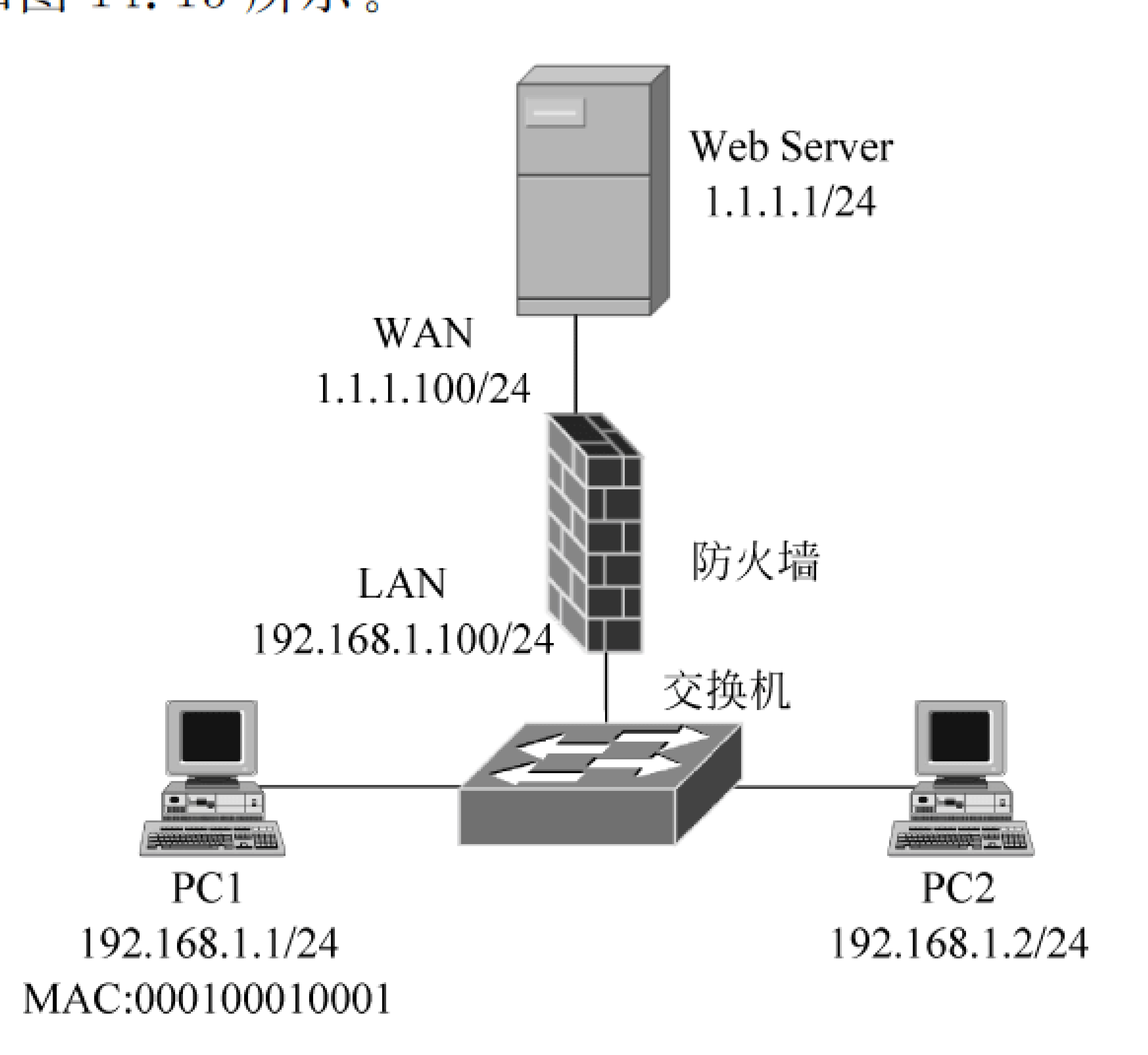


图 14.13 地址绑定实验拓扑

14.4.3 实验原理

如果防火墙某网口配置了 IP/MAC 地址绑定功能，并设置了默认策略(允许或禁止)后，当该网口接收数据包时，防火墙将根据数据包中的源 IP 地址与源 MAC 地址，检查管理员设置好的 IP/MAC 地址绑定表。如果地址绑定表中查找成功，匹配则允许数据包通过，不匹配则禁止数据包通过。如果查找失败，则按默认策略(允许或禁止)执行。

14.4.4 实验步骤

(1) 按照拓扑正确配置防火墙接口和 PC 的 IP 地址，具体如表 14.1 所示。

(2) 进入防火墙配置页面，选择"安全策略"→"地址绑定"，首先启用 LAN 接口的 IP/MAC 绑定功能，并设置默认策略为允许，即如果为查找到 IP/MAC 绑定条目，则允许数据包通过。配置完成后单击"确定"按钮，如图 14.14 所示。

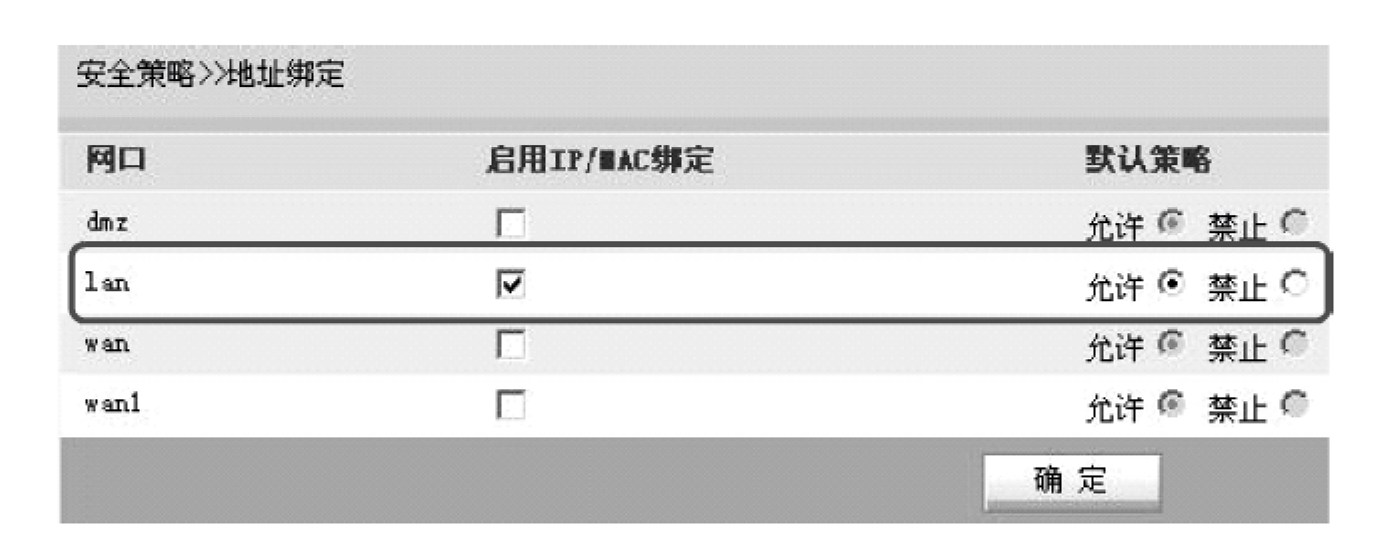


图 14.14 地址绑定

(3) 单击页面中的"添加"按钮，如图 14.15 所示。为 PC1 手工添加 IP/MAC 地址绑定条目(假设 PC1 的 MAC 地址为 00-01-00-01-00-01)，如图 14.16 所示。



图 14.15 添加绑定



图 14.16 设置地址绑定

14.4.5 验证测试

在 PC1 上执行 ping 1.1.1.1,可 ping 通。更改 PC1 的地址为 192.168.1.10,再次执行 ping 1.1.1.1,则无法 ping 通。

14.5 防火墙实现访问控制

14.5.1 背景描述

某学院老师发现,学院内的学生经常利用上课时间浏览新闻网站、QQ 聊天、在线看电影等。老师要求网管针对该问题提供网络解决方案,严格限制学生上课时间随意上网的情况。

14.5.2 实验拓扑

实验的拓扑结构如图 14.17 所示。

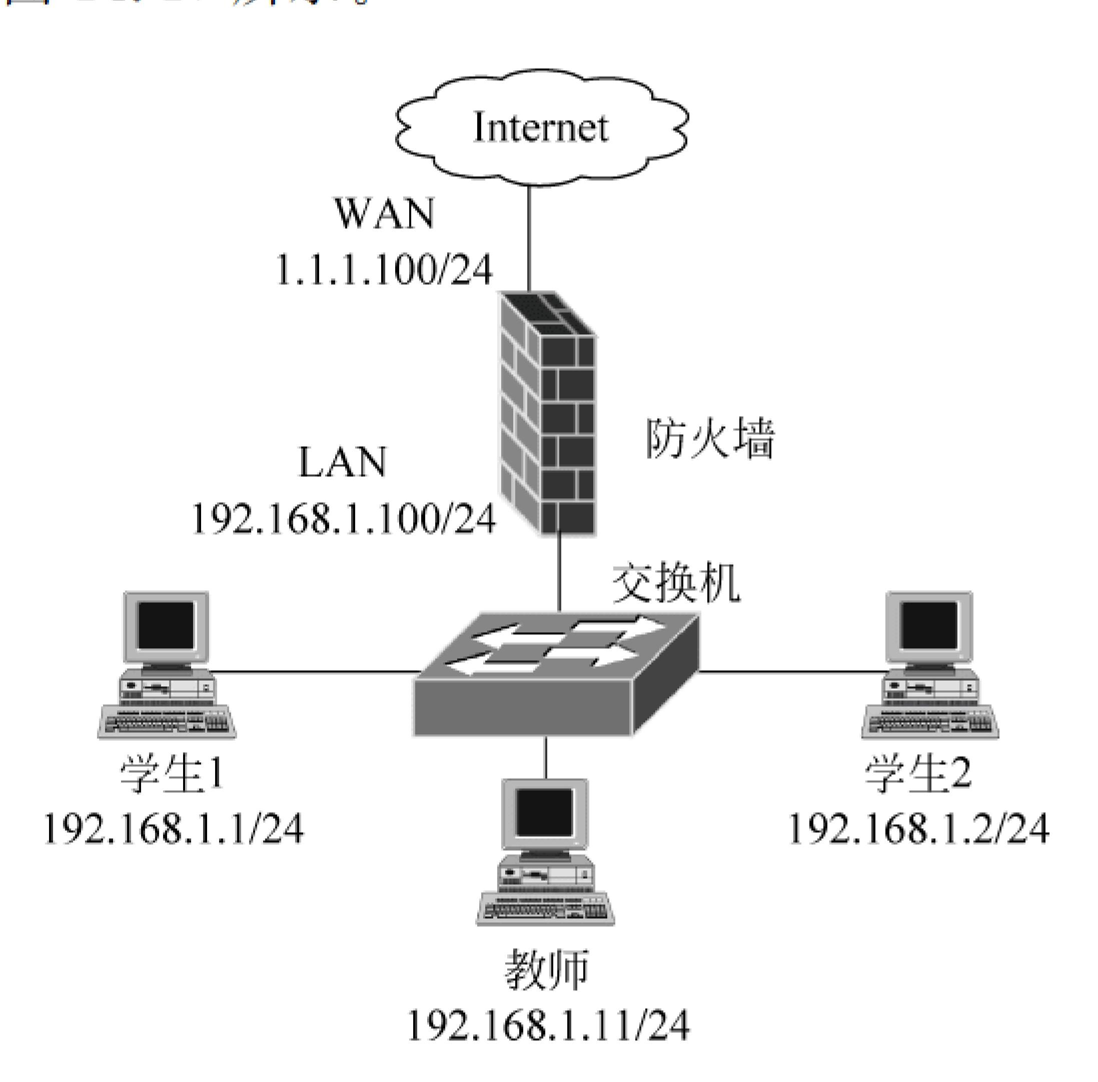


图 14.17 访问控制实验拓扑

14.5.3 实验原理

访问控制是防火墙的基本功能,可以基于 IP 地址、服务端口、时间、域名等因素进行严格的访问控制。

14.5.4 实验步骤

(1) 正确配置防火墙和 PC 的 IP 地址,具体如表 14.2 所示。

(2) 定义安全规则,配置教师的 IP 不限时间允许访问任意服务。进入防火墙配置页面,选择"安全策略"→"安全规则",配置包过滤规则,如图 14.18 所示。

表 14.2 IP 规划表

设备名称	IP 地址	子网掩码	默认网关
学生 1	192.168.1.1	255.255.255.0	192.168.1.100
学生 2	192.168.1.2	255.255.255.0	192.168.1.100
教师	192.168.1.11	255.255.255.0	192.168.1.100
防火墙 LAN	192.168.1.100	255.255.255.0	192.168.1.100
防火墙 WAN	1.1.1.100	255.255.255.0	1.1.1.100



图 14.18 包过滤规则

(3) 进入防火墙配置页面,选择“对象定义”→“时间”→“时间列表”,创建包括上课时间的时间对象,如图 14.19 所示。

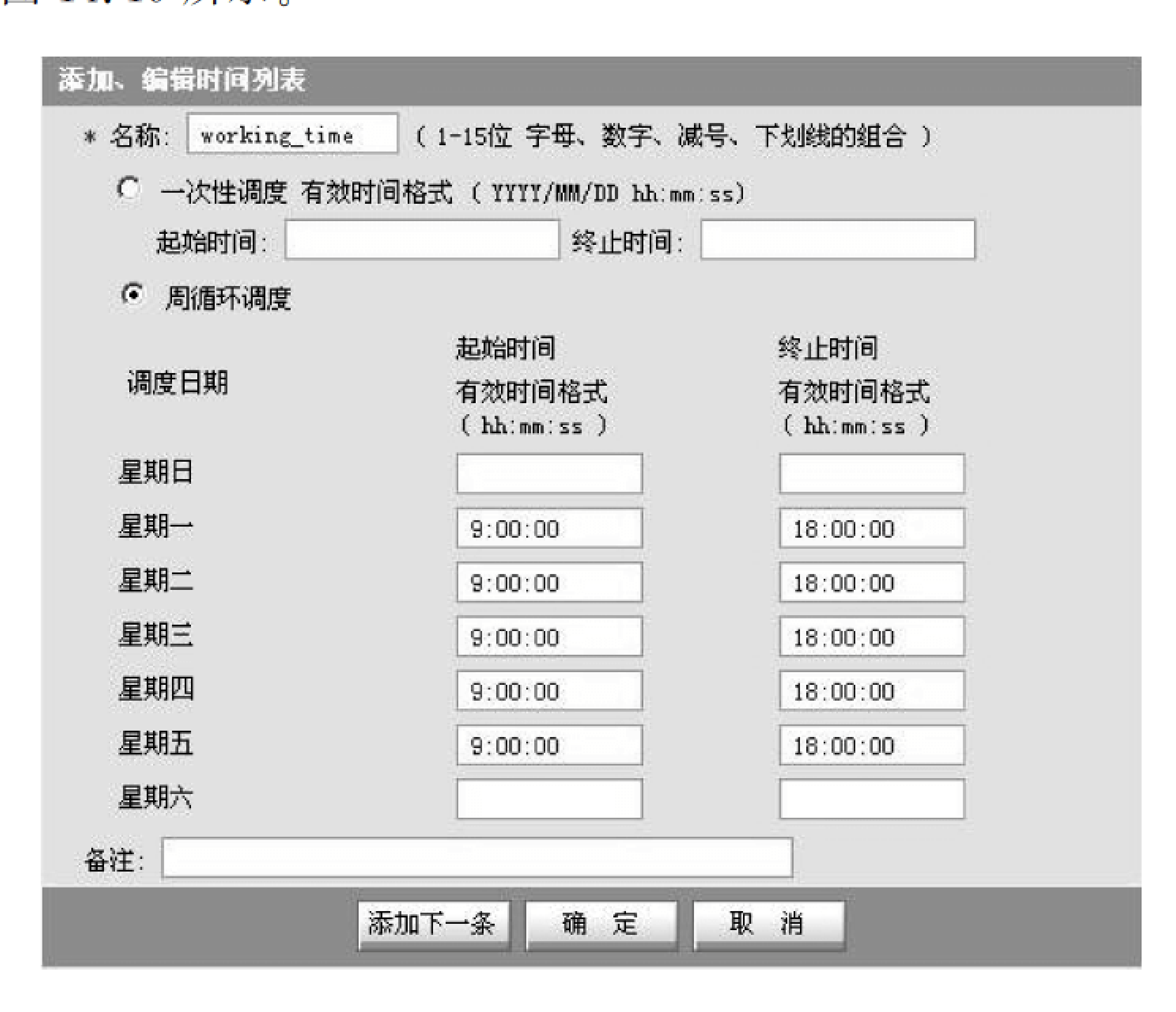


图 14.19 配置时间列表

(4) 定义安全规则,限制学生在上课时间不能访问 Internet。

进入防火墙配置页面,选择"安全策略"→"安全规则",配置包过滤规则,在"时间调度"中选择之前创建的时间对象,过滤动作选择"禁止",如图 14.20 所示。

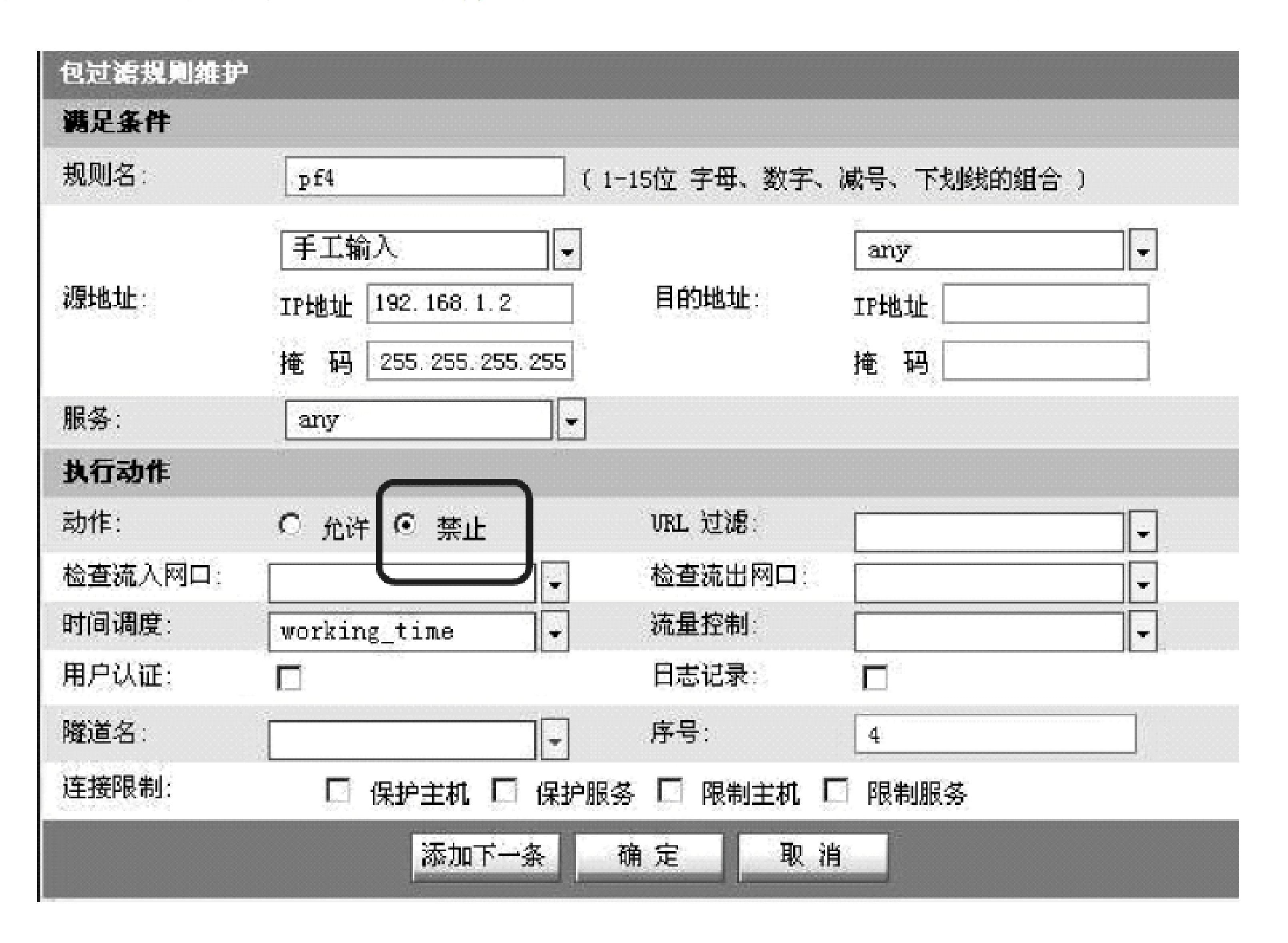


图 14.20 选择"禁止"

(5) 定义最后匹配的安全规则,允许所有访问通过,即满足课余时间无限制地访问。进入防火墙配置页面,选择"安全策略"→"安全规则",配置包过滤规则,如图 14.21 所示。



图 14.21 允许所有访问

14.5.5 验证测试

(1) 老师任何时间可以做任何访问。

(2) 学生上课时间不能访问其他网站。

(3) 学生在下课时间可以访问任意网站的任意服务。

14.6 防火墙实现服务保护

14.6.1 背景描述

某学院使用防火墙作为网络出口设备，并且在防火墙的 DMZ 区域中部署了一台提供对外服务的 Web 服务器。但网络管理员经常发现有大量的到达服务器的连接，致使消耗了服务器大量的系统资源，使其不能提供良好的服务。为了使 Web 服务器正常提供服务，需要保护服务器的系统资源，限制到达服务器的连接数。

14.6.2 实验拓扑

实验的拓扑结构如图 14.22 所示。

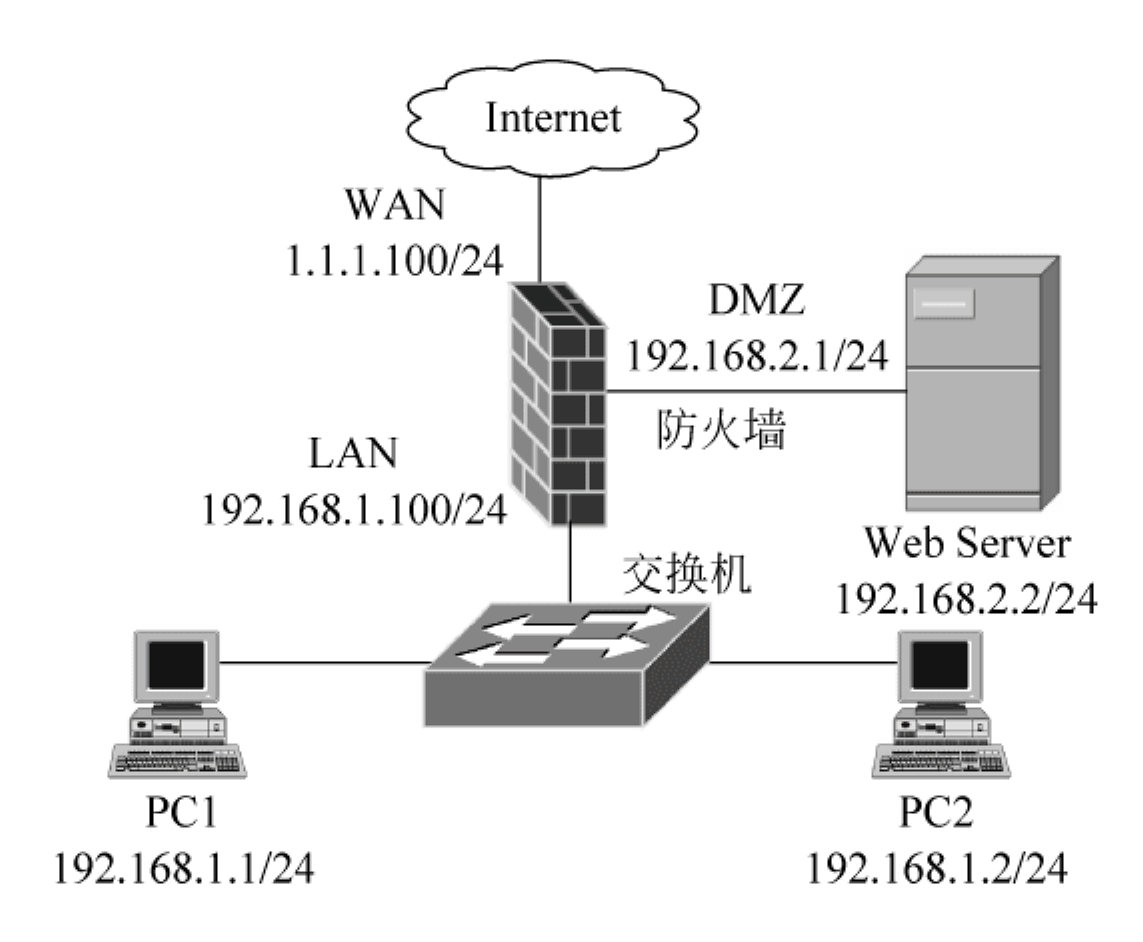


图 14.22 服务保护实验拓扑

14.6.3 实验原理

保护服务是防火墙的一种安全功能，可以限制从公网到达内部网络中主机或服务器的连接数。

14.6.4 实验步骤

(1) 按照拓扑图正确配置防火墙及 Web 服务器的 IP 地址，具体如表 14.3 所示。

表 14.3 IP 规划表

设 备 名 称	IP 地址	子 网 掩 码	默 认 网 关
PC1	192.168.1.1	255.255.255.0	192.168.1.100
PC2	192.168.1.2	255.255.255.0	192.168.1.100
Web Server	192.168.2.2	255.255.255.0	192.168.2.1
防火墙 LAN	192.168.1.100	255.255.255.0	192.168.1.100
防火墙 WAN	1.1.1.100	255.255.255.0	1.1.1.100
防火墙 DMZ	192.168.2.1	255.255.255.0	192.168.2.1

（2）配置连接限制。进入防火墙配置页面，选择“对象定义”→“连接限制”→“保护服务”。单击“添加”按钮，添加规则。如图 14.23 所示，配置为：到达 Web 服务器 192.168.2.2 的并发连接数量达到 50 个时，防火墙不再允许新的连接请求通过。



图 14.23　限制并发连接

（3）定义端口映射规则，使防火墙将 DMZ 中的 Web 服务器发布到公网中。进入防火墙配置页面，选择“安全策略”→“安全规则”→“端口映射规则”。在此规则中选中“保护服务”复选框，以启用此规则的服务保护功能，如图 14.24 所示。



图 14.24　定义端口映射

14.6.5　验证测试

观察从公网到达 Web 服务器的连接，连接数将不能超过 50 个。

14.7　防火墙实现抗攻击

14.7.1　背景描述

某学院老师发现经常有外部的 IP 地址发送大量的数据包对内部网络进行扫描攻击，要求在防火墙上制止这些攻击。

14.7.2　实验拓扑

实验的拓扑结构如图 14.25 所示。

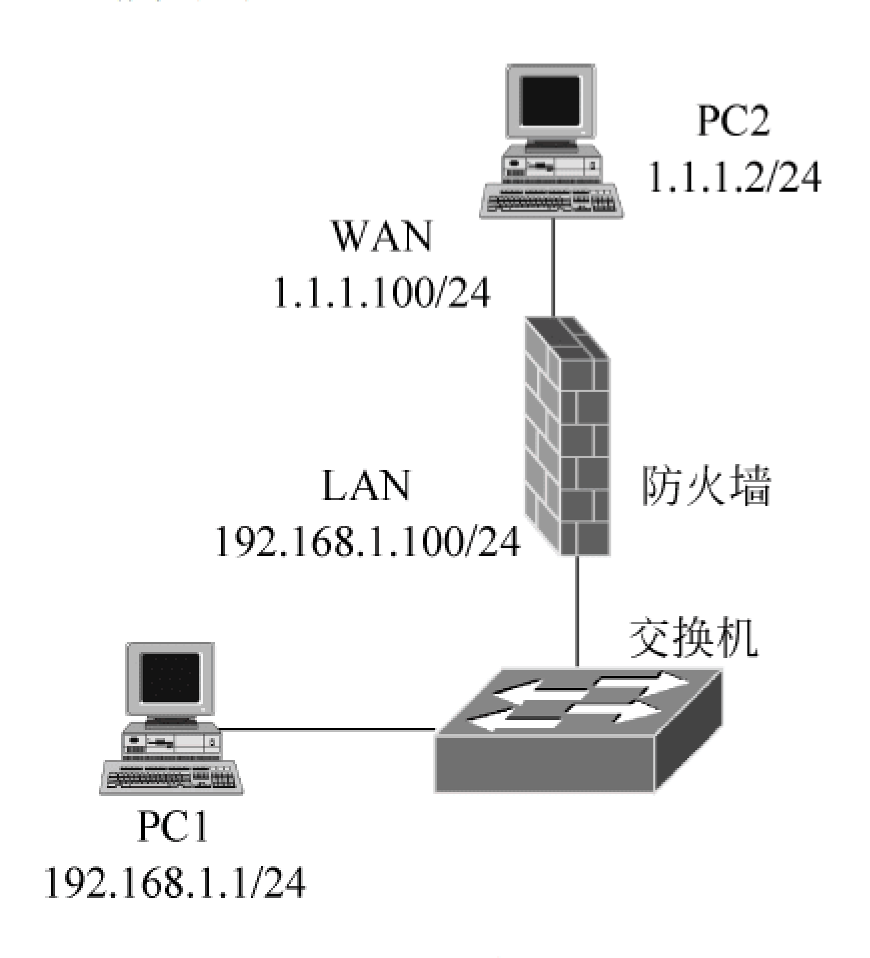


图 14.25　抗攻击实验拓扑

14.7.3　实验原理

防火墙的抗攻击功能可以有效发现并制止网络攻击，从而达到保护内部资源的目的。

14.7.4　实验步骤

(1) 正确配置防火墙和 PC 的 IP 地址，具体如表 14.4 所示。

表 14.4　IP 规划表

设备名称	IP 地址	子网掩码	默认网关
PC1	192.168.1.1	255.255.255.0	192.168.1.100
PC2	1.1.1.2	255.255.255.0	1.1.1.100
防火墙 LAN	192.168.1.100	255.255.255.0	192.168.1.100
防火墙 WAN	1.1.1.100	255.255.255.0	1.1.1.100

(2) 定义安全规则，允许所有访问通过。进入防火墙配置页面，选择“安全策略”→“安全规则”，配置包过滤规则，如图 14.26 所示。

(3) 配置防火墙 WAN 接口的抗攻击功能。进入防火墙配置页面，选择“安全策略”→“抗攻击”，选择 WAN 接口，如图 14.27 所示。



图 14.26　配置包过滤规则

安全策略>>抗攻击

接口名称	启用	SYN Flood	ICMP Flood	Ping of Death	UDP Flood	PING SWEEP	TCP端口扫描	UDP端口扫描	WinNuke	操作
dmz	✖	✖	✖	✖	✖	✖	✖	✖	✖	📝
lan	✖	✖	✖	✖	✖	✖	✖	✖	✖	📝
wan	✖	✖	✖	✖	✖	✖	✖	✖	✖	📝
wan1	✖	✖	✖	✖	✖	✖	✖	✖	✖	📝

图 14.27　抗攻击设置

（4）启用“抗攻击功能”，并开启端口扫描攻击，如图 14.28 所示。



图 14.28　开启抗攻击

14.7.5 验证测试

在启动抗攻击前，在 PC2 上使用端口扫描工具对 PC1 进行扫描，发现 PC1 的接口接收到大量的数据包，即 PC2 的扫描工具发送的报文，且扫描工具正确扫描到 PC1 上已开放的端口。在启动抗攻击后，在 PC2 上使用端口扫描工具对 PC1 进行扫描，发现 PC1 的接口只接收到少数几个数据包，其他大量的扫描数据包已经被防火墙阻拦，且在 PC2 的扫描工具不能扫描到 PC1 上开放的端口。

14.8 防火墙实现链路负载

14.8.1 背景描述

某学校信息中心原来有一条 10Mb/s 线路，最近新申请了一条 10Mb/s 线路，要求防火墙同时使用新旧两条线路，并且将流量合理分摊。

14.8.2 实验拓扑

实验的拓扑结构如图 14.29 所示。

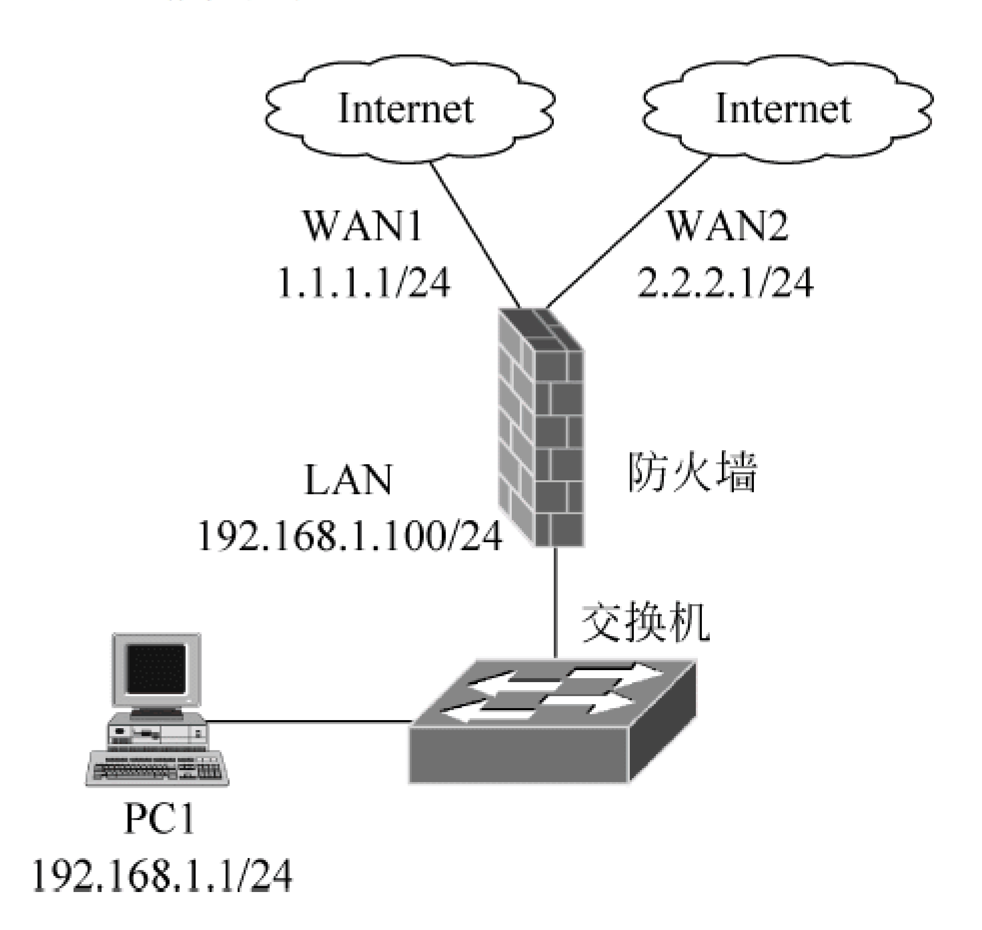


图 14.29 链路负载实验拓扑

14.8.3 实验原理

通过两条链路，为两个路由下一跳配置相应的权重，合理分配网络流量。

14.8.4 实验步骤

(1) 正确配置防火墙和 PC 的 IP 地址，具体如表 14.5 所示。

(2) 定义安全规则，允许所有访问通过。进入防火墙配置页面，选择“安全策略”→“安全规则”，配置包过滤规则，如图 14.30 所示。

(3) 定义策略路由。进入防火墙配置页面，选择“网络配置”→“策略路由”，单击“添加”按钮，配置到公网的路由，并配置两个下一跳地址，分配相等的权重，即保证流量平分到两条链路上，如图 14.31 所示。

表 14.5　IP 规划表

设 备 名 称	IP 地址	子 网 掩 码	默 认 网 关
PC1	192.168.1.1	255.255.255.0	192.168.1.100
防火墙 LAN	192.168.1.100	255.255.255.0	192.168.1.100
防火墙 WAN1	1.1.1.1	255.255.255.0	1.1.1.1
防火墙 WAN2	2.2.2.1	255.255.255.0	2.2.2.1

包过滤规则维护
满足条件
规则名：pf1 （1-15位 字母、数字、减号、下划线的组合）
源地址：any IP地址 掩 码
目的地址：any IP地址 掩 码
服务：any
执行动作
动作：允许 禁止
URL 过滤：
检查流入网口：
检查流出网口：
时间调度：
流量控制：
用户认证：
日志记录：
隧道名：
序号：3
连接限制：保护主机 保护服务 限制主机 限制服务
添加下一条 确 定 取 消

图 14.30　允许所有访问



图 14.31　配置策略路由

实验思考题

1. 实验中你都学到了哪些内容？
2. 硬件防火墙有哪些登录验证方式？
3. 如何限制常用的网络功能，例如 FTP、BT、QQ 等。
4. 如果配置中有两条规则是互相矛盾，例如前一条是禁止某个端口，后一条是打开这个端口，请问会出现什么情况？
5. 利用 Web 和超级终端登录分别有哪些优缺点？

第15章 实验6 VPN设备的使用与配置

15.1 实验目的及要求

15.1.1 实验目的

掌握 VPN 设备的基本使用原理,学习通过 Console 口进行系统配置,学习 IPSec VPN 隧道,熟悉移动办公方式下的 VPN 隧道建立,学习采用 USB Key 的数字证书方式进行用户身份认证。

15.1.2 实验要求

根据教材中介绍的操作步骤完成实验内容,详细观察并记录设置的内容,理解设置的内容和原理,做出分析并写出实验总结报告。

15.1.3 实验设备及软件

VPN 设备 RG-WALL V50 1 台、VPN 远程接入系统 RG-SRA 1 套、路由器设备 1 台、PC 2 台。

15.1.4 实验拓扑

实验的拓扑结构如图 15.1 所示。

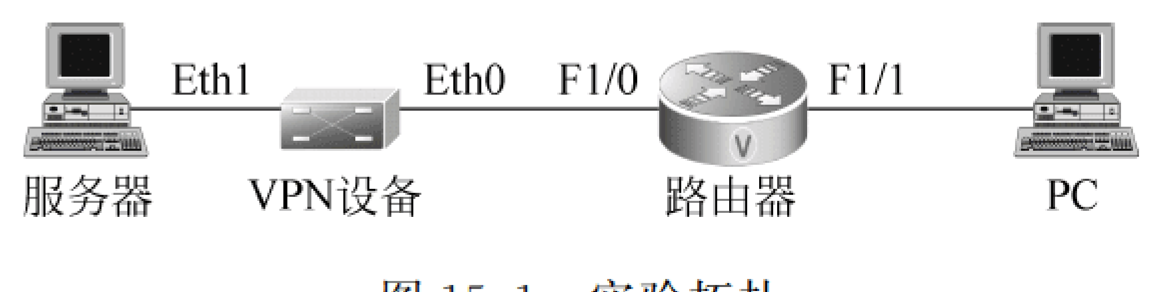


图 15.1 实验拓扑

15.2 锐捷 VPN 命令行操作

15.2.1 系统管理模式

锐捷 VPN 网关采用分级管理模型,管理员分为两级:串口管理员、界面管理员,并各自拥有不同的权限。

串口管理员负责对 VPN 网关的基本配置,并可以设置修改界面管理员的口令,并限制

界面管理员登录的 IP 地址。一般在初始配置完成后，只要网络的拓扑结构不再修改，无需再进行串口配置。

界面管理员则负责 VPN 网关日常的管理和配置，如具体的访问控制规则、隧道监控等。

15.2.2 管理员

锐捷 VPN 网关安装后，串口管理员 sadm 必须通过 Console 口进行系统配置，包括设定 VPN 网关的 IP、路由、域名服务器、接口配置、用户管理等。

sadm 的出厂默认口令为 sadm。

串口管理员 sadm 和界面管理员 adm 不能同时登录，当 adm 用户登录到 GUI 管理界面上时，串口只能用 sadmview 用户来查看配置，sadmview 不能修改配置，出厂口令为 sadmview。

15.2.3 串口管理

首先要对安全网关进行最基本的网卡、路由和管理员等信息的配置。进行配置时使用便携机或台式机通过串口线与安全网关设备的串口相连，在 Windows 9x/2000 或 Windows XP 下运行“开始”菜单中的“程序”→“附件”→“通信”→“超级终端”程序。

“连接时使用”串口按默认值，一般为 COM1，具体串口根据控制台机器的串口线连在哪个串口上为准。设置连接速率“每秒位数”为 9600，其他为默认值，即可连接到安全网关上。

在使用超级终端时，若要使 Backspace 退格键有效，需在超级终端的菜单栏“文件”处选择“属性”，然后单击“设置”按钮，将“Backspace 键发送”这一栏选为 Del(D)。

clear(cl)命令为清空系统当前所有配置恢复到出厂设置。

```
[sadm@RG-WALL]# clear conf 输入命令 clear conf 清空配置
Warning: The command will restore all
system configuration to default and then
REBOOT the system!!!
Are you sure to CLEAR all the system
configuration and REBOOT
system? (Y/N):n
警告：是否要清空所有配置，恢复到出厂设置并重新启动操作系统 Y：确认、N：否。
```

15.3 IPSec VPN 通信实验

15.3.1 设备的初始化设置

(1) 准备好 PC 和服务器

在服务器上安装 VPN 管理软件，通过服务器管理 VPN 设备，在 PC 上安装 RG-SRA

软件，RG-SRA 软件是 VPN 客户端程序。

(2) 搭建实验拓扑如图 15.1 所示，然后配置各设备数据如表 15.1 所示。

表 15.1 IP 规划表

设备名称	IP 地址	子网掩码	默认网关
VPN 的 Eth1(WAN)	192.168.1.1	255.255.255.0	192.168.1.1
VPN 的 Eth0(LAN)	10.1.1.2	255.255.255.0	10.1.1.1
PC	10.1.2.2	255.255.255.0	10.1.2.1
服务器的 IP	192.168.1.2	255.255.255.0	192.168.1.1
路由器 f1/0	10.1.1.1	255.255.255.0	
路由器 f1/1	10.1.2.1	255.255.255.0	

(3) 设置路由器的 IP 地址(以锐捷路由器为例)，如下所示：

```
Router>en
Router#conf t
RouterA(config)#interface f1/0 ! 进入路由器的快速以太网端口 F1/0
RouterA(config-if)#ip address 10.1.1.1 255.255.255.0
RouterA(config-if)#no shutdown
RouterA(config-if)#exit
RouterA(config)#interface f1/1 ! 进入路由器的快速以太网端口 F1/1
RouterA(config-if)#ip address 10.1.2.1 255.255.255.0
RouterA(config-if)#no shutdown
RouterA(config-if)#exit
RouterA#show ip interface f1/0
RouterA#show ip interface f1/1
```

15.3.2 VPN 管理器的安装

锐捷 VPN 管理平台是一个基于 Windows 图形用户界面的管理工具。目前锐捷 VPN 管理平台支持 Windows 系列的各种中文操作系统，如 Win98、Win2000 系列、Win XP、Win2003 等。锐捷 VPN 管理平台可以同时对多台不同版本的 VPN 设备进行集中管理。安装程序直观简洁，一步一步按照提示，直接采用默认设置，用户就可以轻松地完成锐捷 VPN 管理平台的安装。具体步骤如下：

(1) 双击锐捷网关管理中心软件安装包(锐捷网关管理中心_2.30.10.exe)，打开 VPN 管理平台安装界面，如图 15.2 所示。

(2) 在图 15.2 中单击“下一步”按钮，进入许可证协议框，选择“接受许可协议”。

(3) 再单击“下一步”按钮，进入 VPN 的安装目录，如图 15.3 所示。

(4) 然后连续单击“下一步”按钮，当弹出图 15.4 所示的界面时，表示已经成功安装了锐捷 VPN 管理平台。



图 15.2　安装欢迎界面



图 15.3　选择安装目标文件夹



图 15.4　安装完成

15.3.3　VPN 首次配置

首先把 VPN 设备通电，VPN 设备出厂时 Eth1 网口有一个默认 IP 地址配置，即 IP 地址：192.168.1.1，子网掩码：255.255.255.0。在配置设备之前，计算机需要一个和设备 Eth1 接口在同一网段的 IP 地址；如果使用计算机直接连到 Eth1 接口，用户可以使用交叉网线；如果把设备的 Eth1 网口直接连到 HUB 或交换机上，请使用直通线。

在计算机能够与设备通信之前，用户必须修改计算机的网络配置。具体操作为：单击“开始”→“设置”→“网络和拨号连接”，双击“本地连接”，再单击“属性”，重新设置一个同一网段的 IP 地址，如图 15.5 所示，设置计算机的 IP 地址为 192.168.1.2。

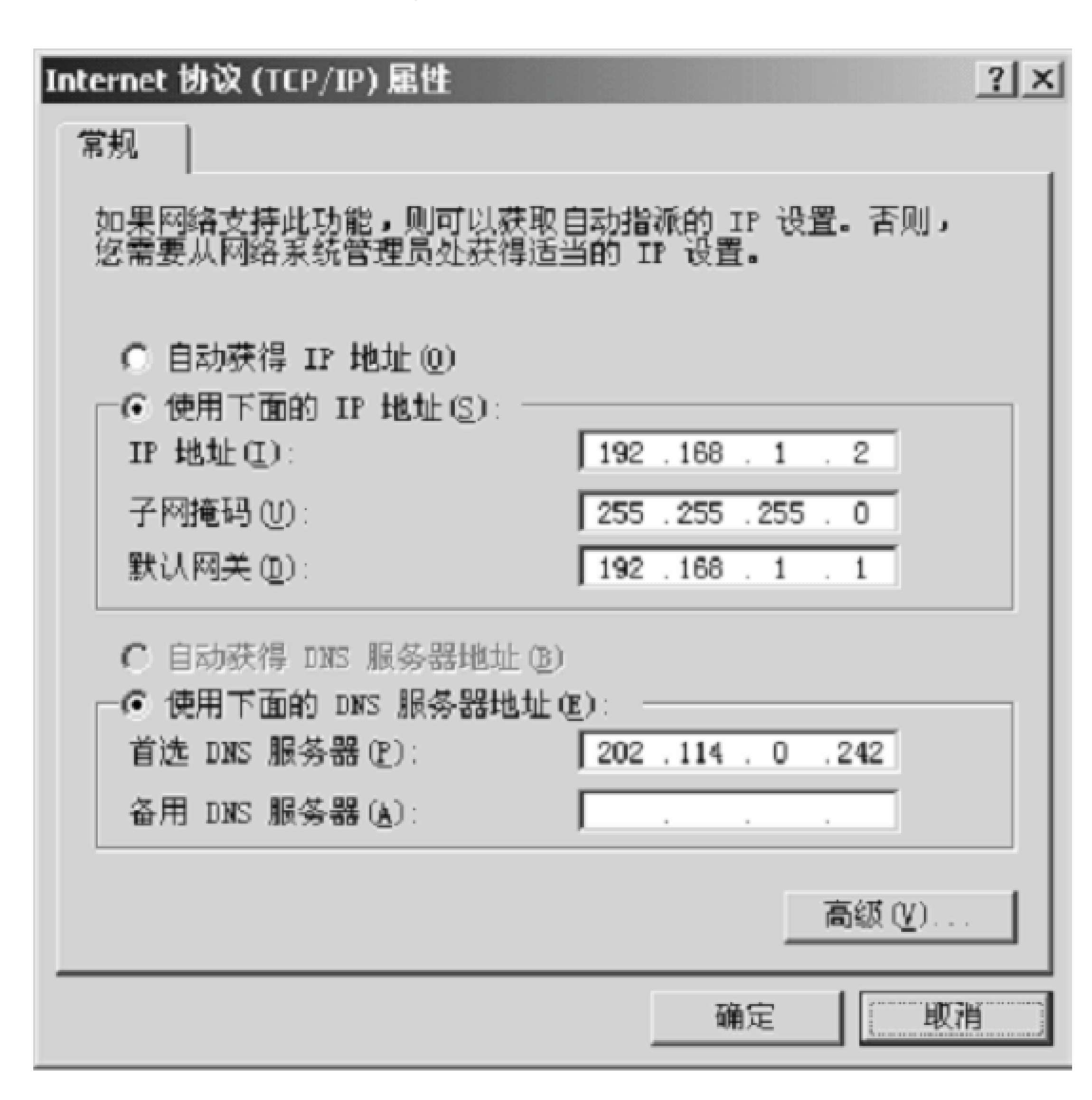


图 15.5　本地 IP 设置

配置好后，就可以从 VPN 管理平台登录到锐捷 VPN 设备了。具体操作为：

(1) 打开“开始”→“程序”→“锐捷 VPN 管理平台”，启动锐捷 VPN 管理平台。若是第一次打开 VPN 管理平台，里面是没有任何 VPN 设备的，需要依次添加网关组与网关。

(2) 可以从“文件(F)”→“新建(N)”→“网关组(G)”，添加一个网关组，如图 15.6 所示。

(3) 添加完网关组后，便可添加网关，从“文件(F)”→“新建(N)”→“网关组(G)”，可以添加网关，在打开的属性框中，填写网关的属性，如图 15.7 所示。



图 15.6　新建网关组

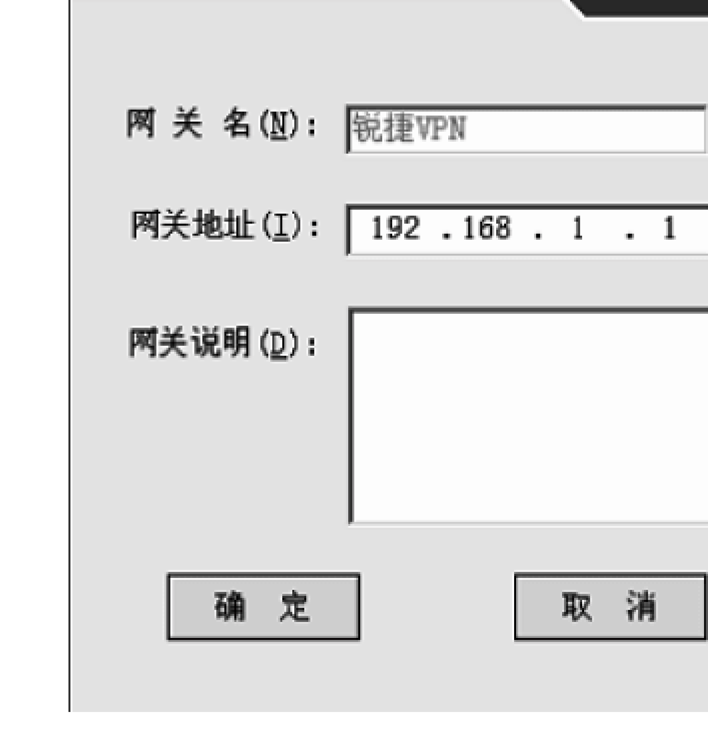


图 15.7　填写网关属性

(4) 填写完成后，单击“确定”按钮，便回到锐捷 VPN 管理平台的主界面，如图 15.8 所示。

15.3.4　VPN 管理平台登录

在锐捷 VPN 管理平台界面中双击要登录的网关，系统将弹出 VPN 的登录框，如图 15.9 所示。设备出厂默认账号是 adm，密码是 adm。管理员可以在用户认证模块中修改密码。

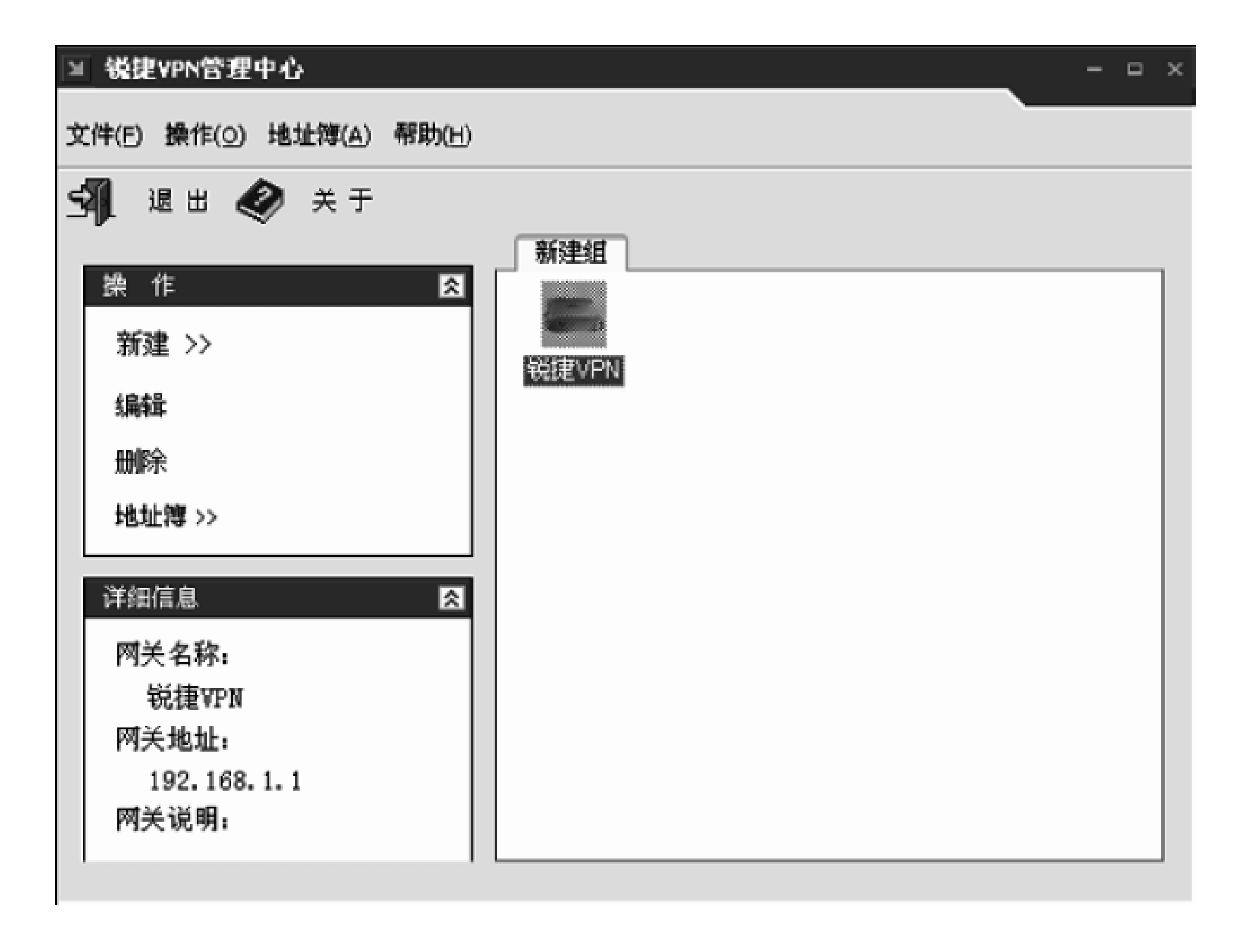


图 15.8　成功添加一个网关



图 15.9　系统登录窗口

若密码填写无误，单击“登录”按钮，便可登录到锐捷 VPN 设备了。登录后的界面如图 15.10 所示。



图 15.10　管理界面

15.3.5　网络接口设置

如果需要对某个物理接口进行设置，那么在网关 VPN 界面右边的目录树上单击“网络配置”选项，双击“网络接口”选项，如图 15.11 所示。

打开设置窗口，主窗口中网络接口列表显示的是网关设备的所有网络接口信息。在网络接口主界面中分为上、下两部分，上面部分是几个对设备支持的物理接口进行操作的按钮，为设置接口、启用接口、停用接口；下面的网络接口状态部分主要列出了每个接口的状态，包括接口名、配置状态、启用状态、连接状态、连接速率、IP 地址等信息。

在网络接口界面上单击设置接口按钮，打开接口设置框，显示的是常规选项卡内的信息，常规选项卡主要是显示该接口基本情况。在配置信息选项卡中，有多种配置方法可以对接口进行配置，如图 15.12 所示，包括自动获得 IP 地址、静态配置、拨号、加入网桥，还可以不对其进行配置，并可对链路的权重进行设置。其中权重在进行多个外出链路的备份和均衡中将起到一定的平衡负载作用。

如果该物理接口属于静态路由接口，那么这里选择的是静态获得 IP 地址，就要在图中输入需要添加接口的 IP 地址和子网掩码以及默认网关。

15.3.6　配置 IPSec VPN 隧道

在虚拟专用网的目录上选择 IPSec VPN 并打开，如果需要配置远程移动用户接入，那

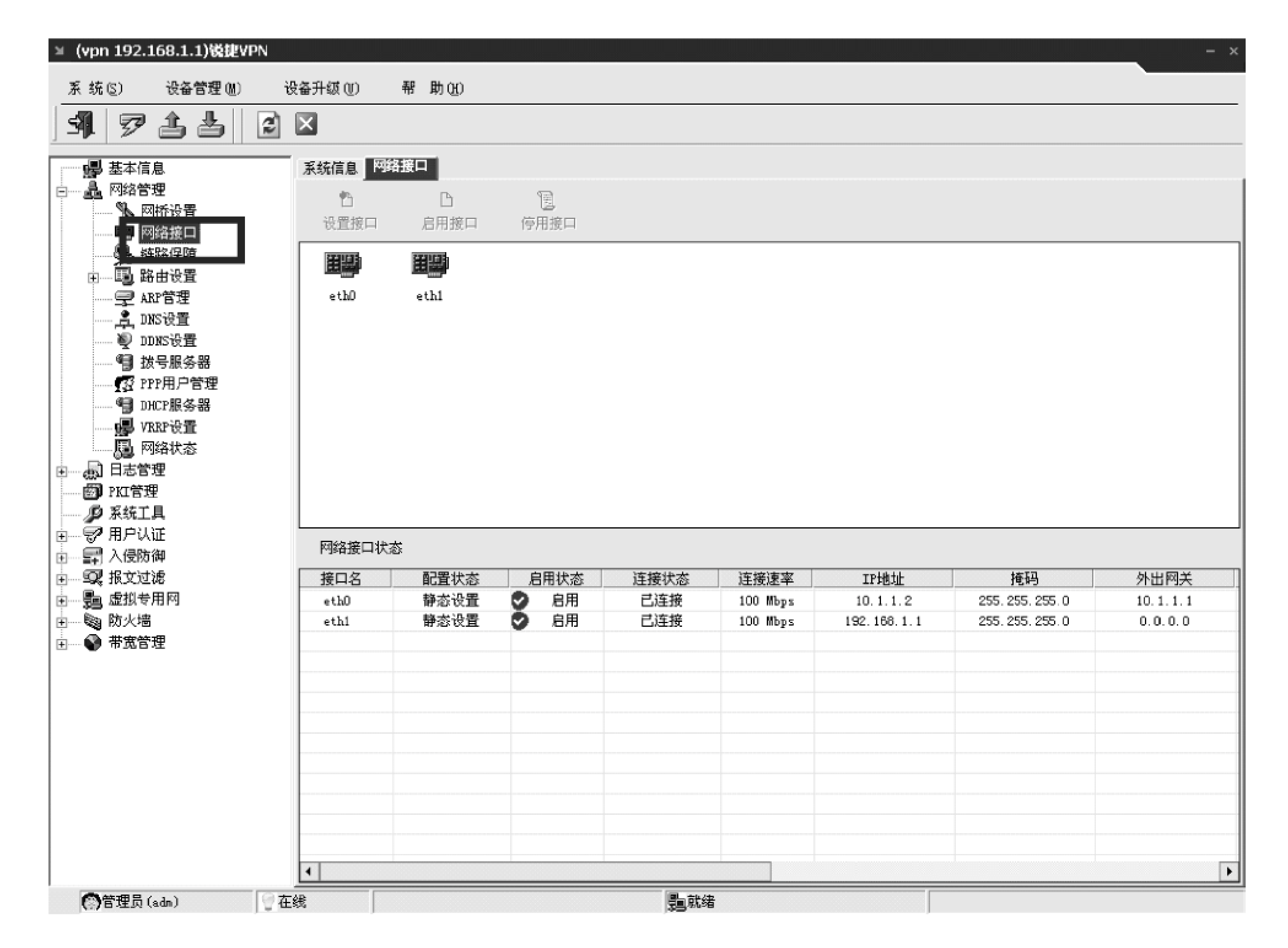


图 15.11　网络接口设置

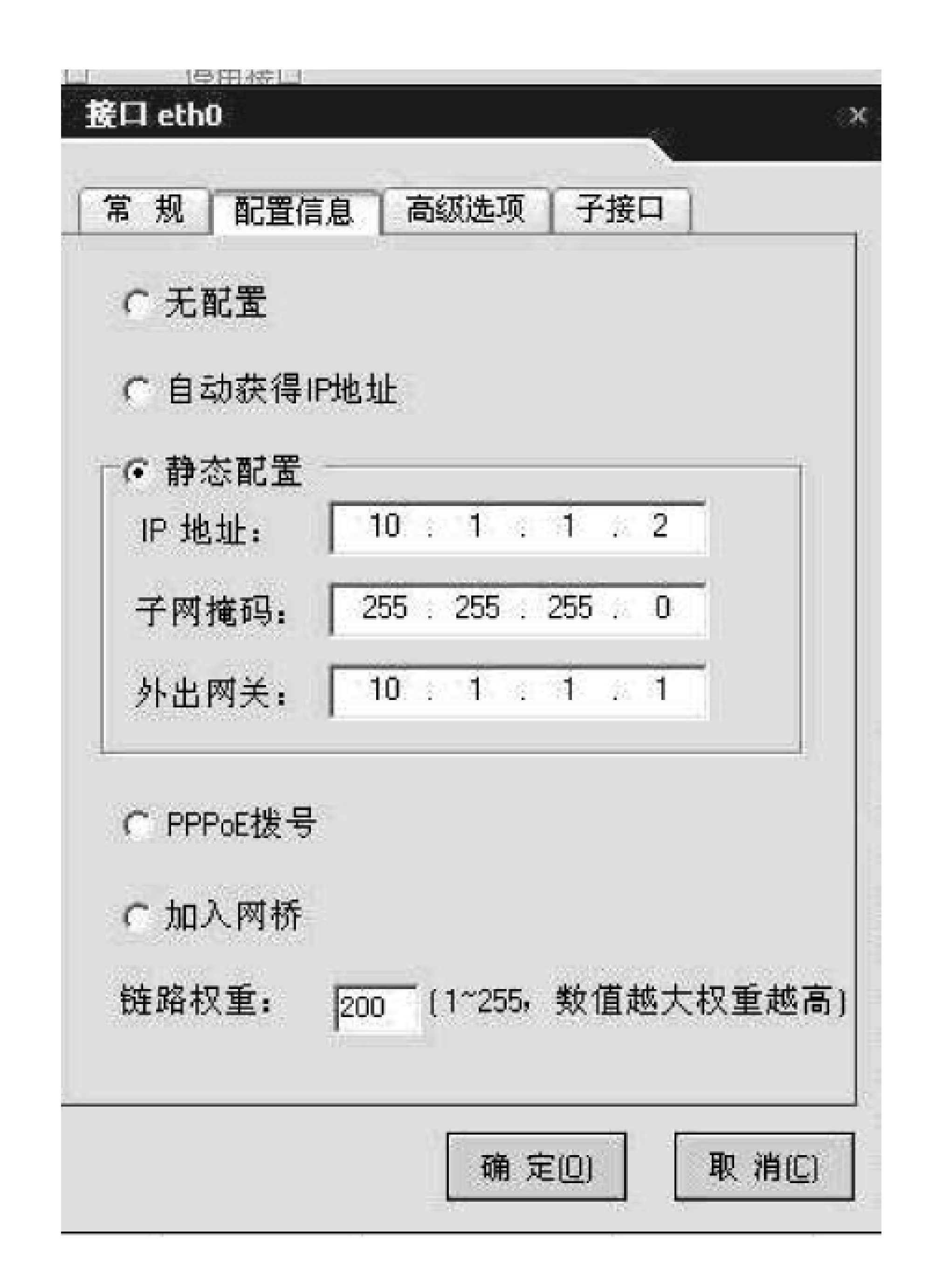


图 15.12　接口设置框

么在图中双击远程用户管理，打开远程用户管理界面，如图 15.13 所示。

允许访问内部子网，设置允许客户端访问的内部子网信息，如图 15.14 所示。

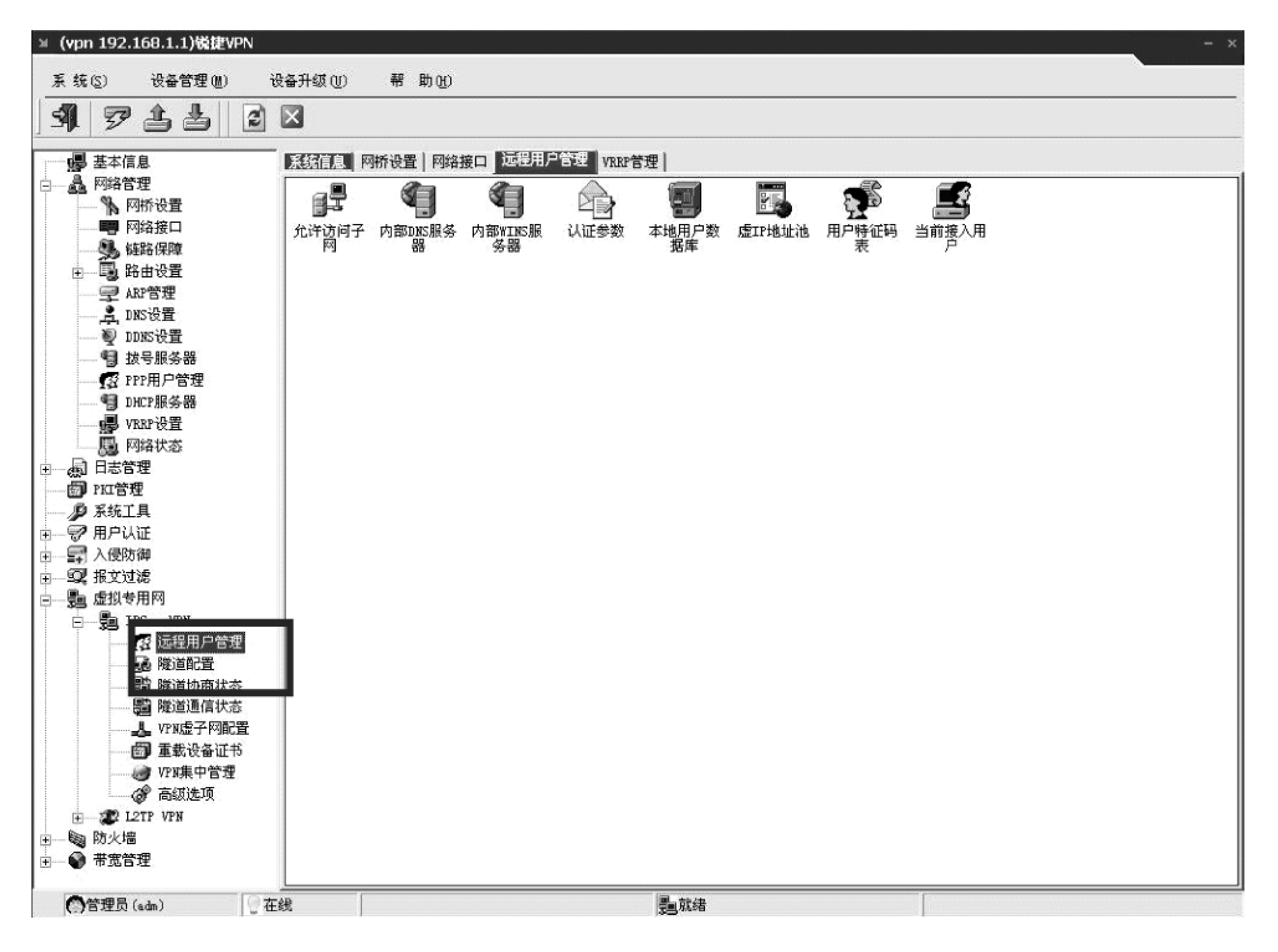


图 15.13 远程用户管理界面

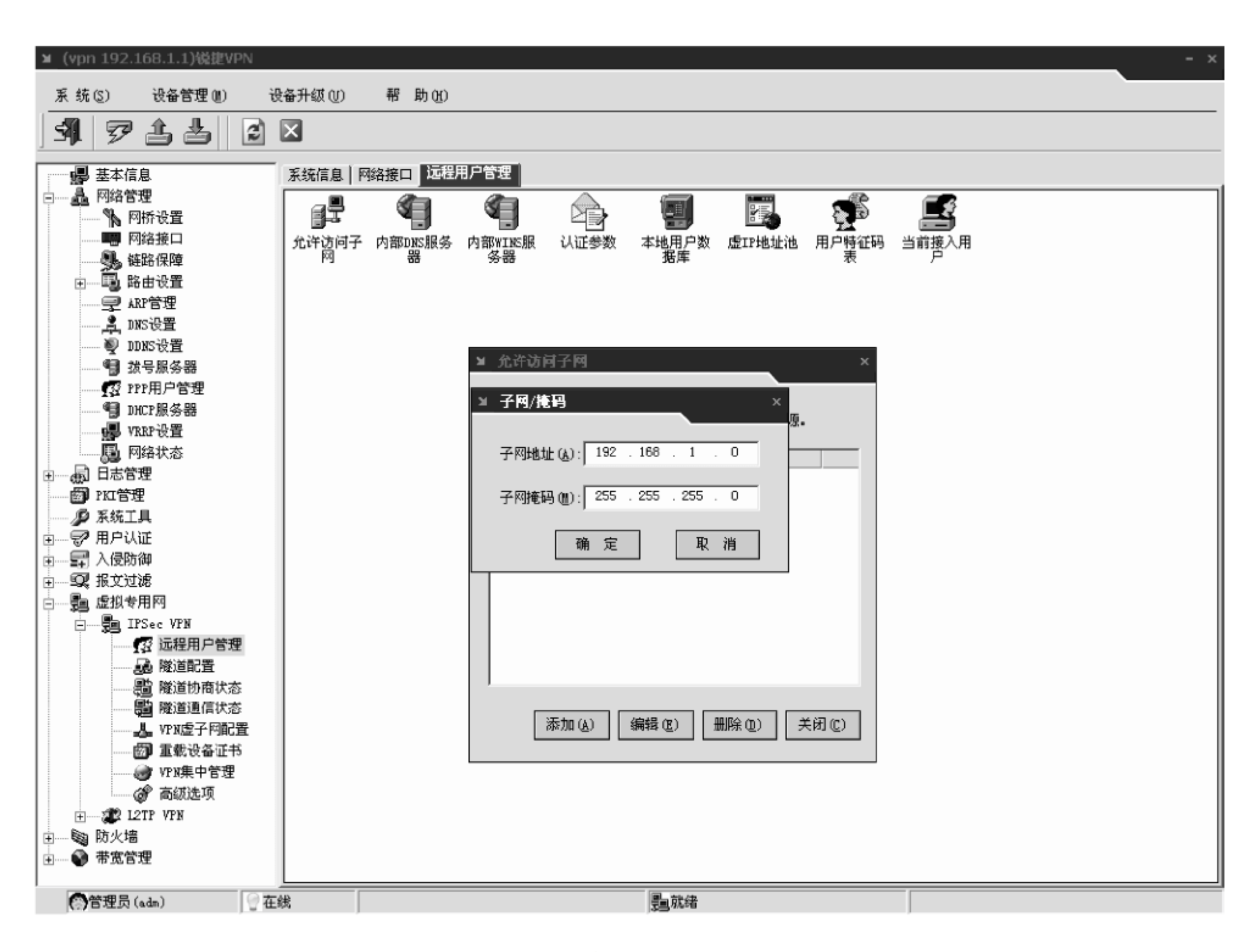


图 15.14 允许访问内部子网设置

内部地址池允许网络管理人员输入一个或者几个 IP 地址范围，这些地址将用于对远程端用户分配虚拟 IP 地址，如图 15.15 所示。

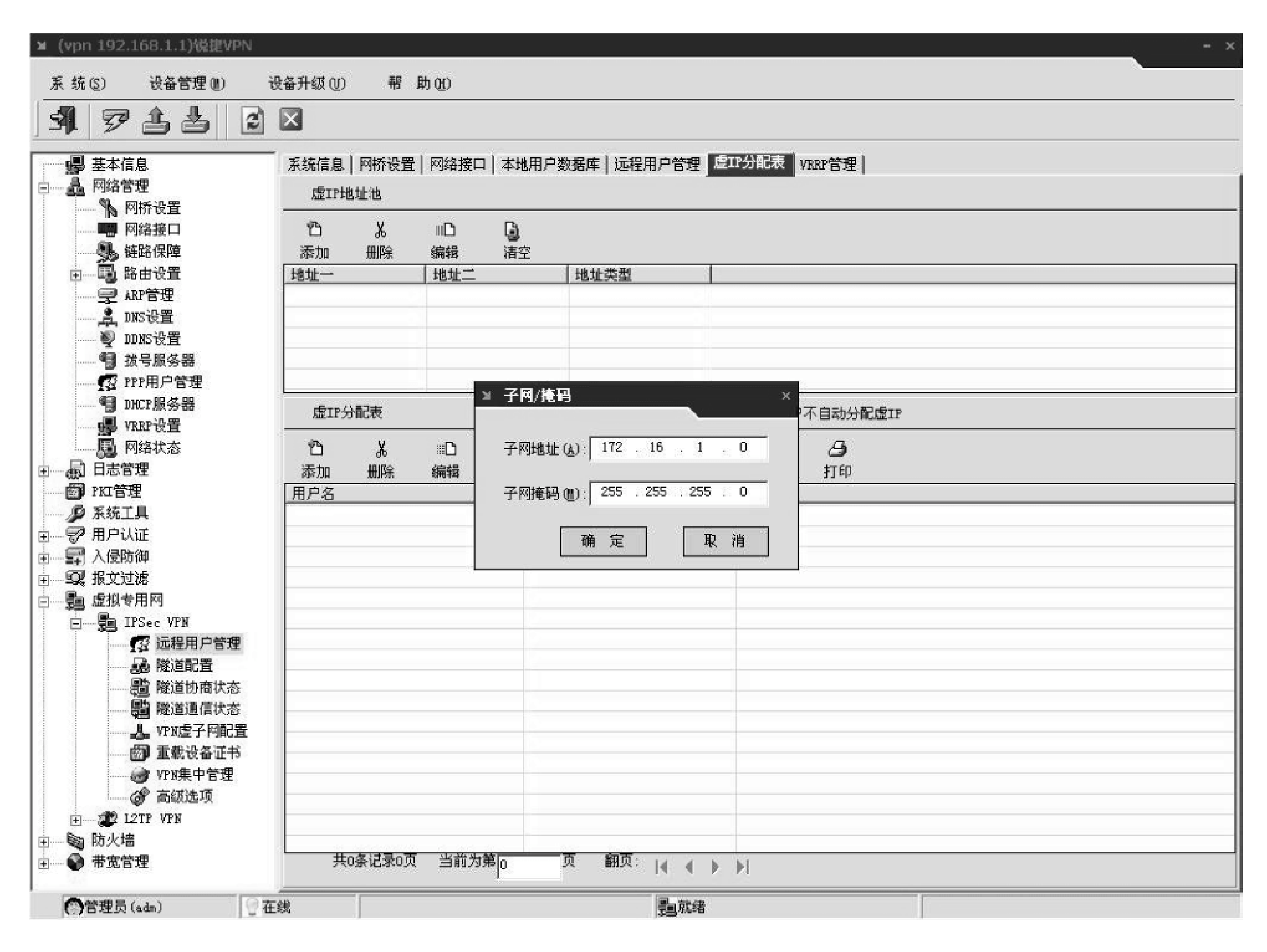


图 15.15 内部地址池设置

配置本地用户数据库，创建一个用户名为 test，密码为 1234，并允许用户登录，如图 15.16 所示。



图 15.16 添加用户

添加完后单击“用户生效”按钮,否则新用户无法使用,如图 15.17 所示。

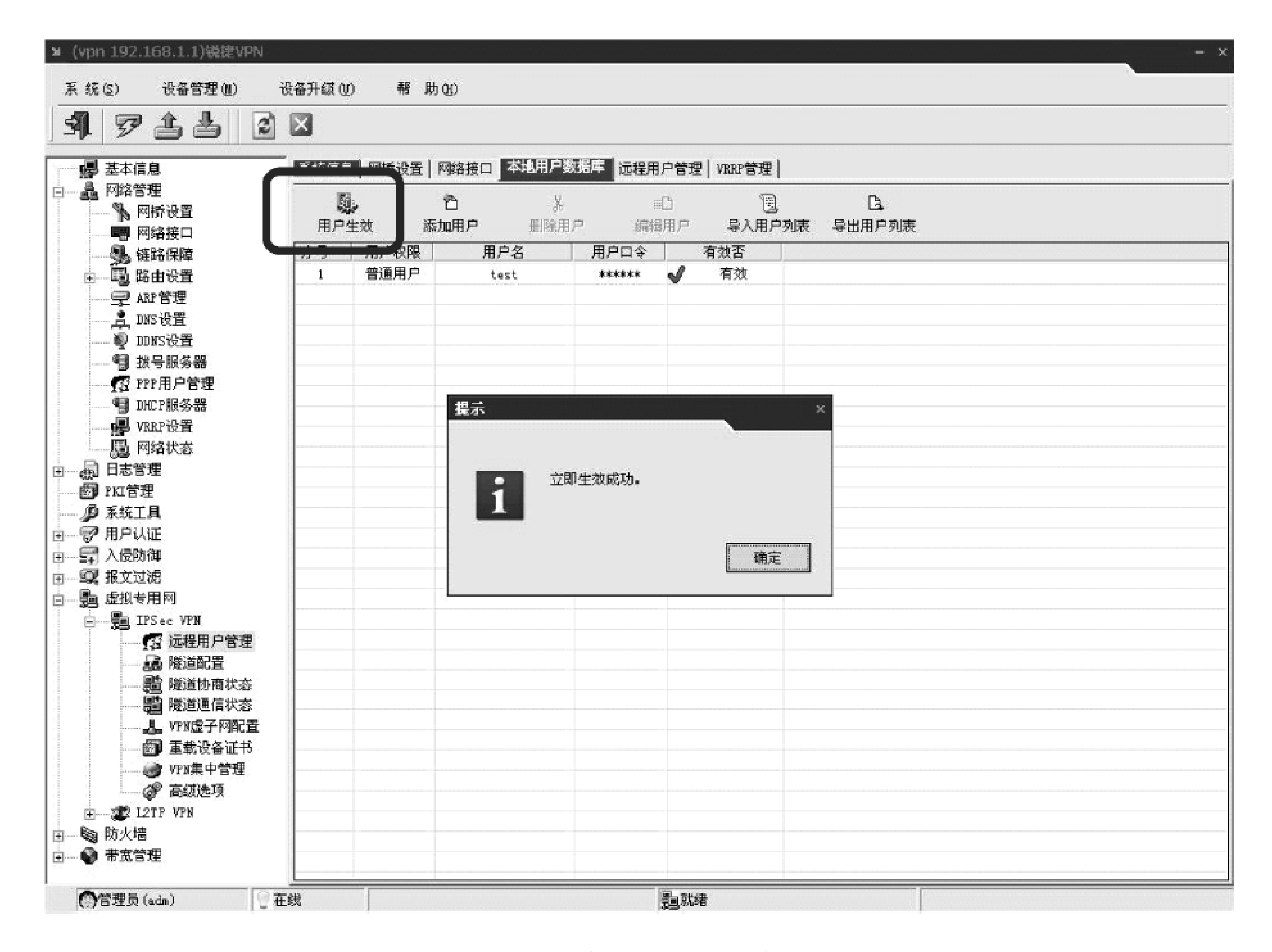


图 15.17　单击“用户生效”按钮

用户特征码表,如果需要对用户的登录机器进行限制,可以对用户机器特征进行绑定,如图 15.18 所示。

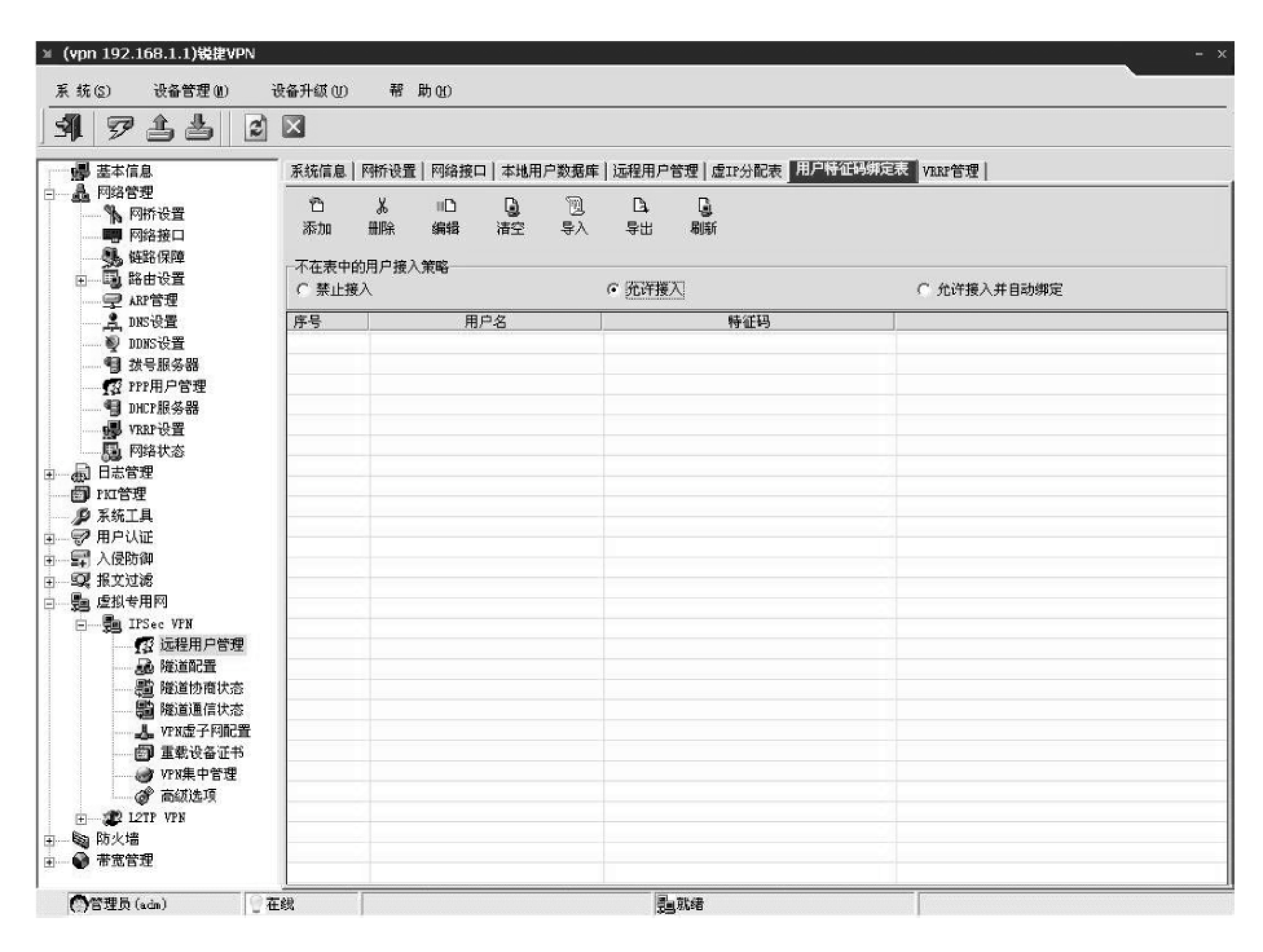


图 15.18　用户特征码表

用户机器的特征(每个客户端软件都可以显示本机的特征码)可以由管理员手工导入，也可以由客户端首次上线的时候自动报告。此外，系统对不在绑定表中的用户接入策略分为三种：禁止接入、允许接入不自动进行绑定特征码、允许接入并自动绑定特征码。

15.3.7　RG-SRA 程序的使用

在客户端 PC 上运行 RG-SRA 程序，开始建立 VPN 隧道，如图 15.19 所示。

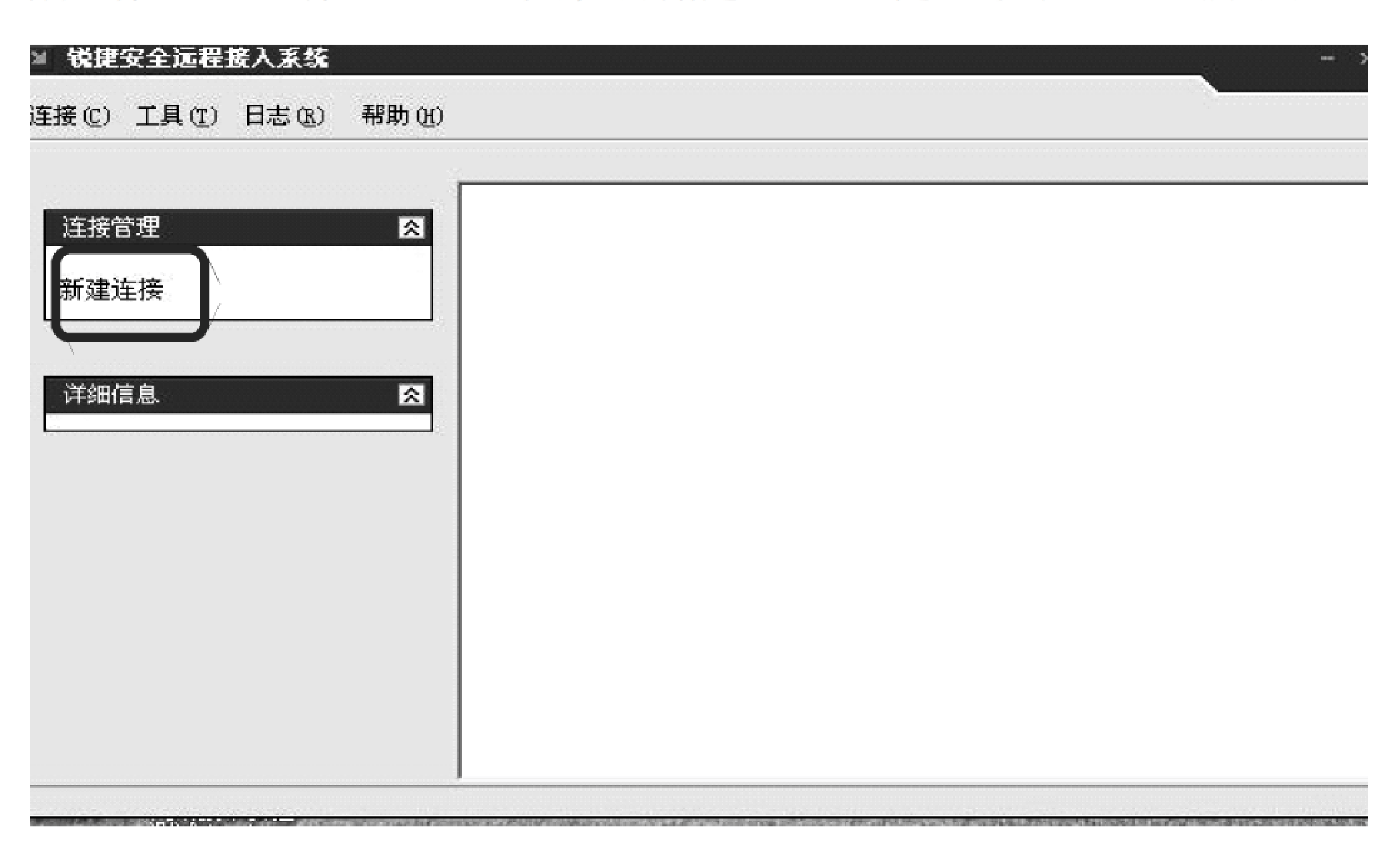


图 15.19　RG-SRA 程序界面

单击“新建连接”按钮，填写如下基本信息，认证方式选择“网关本地认证”，如图 15.20 所示。



图 15.20　新建连接配置

按鼠标右健，启动连接，如图 15.21 所示。

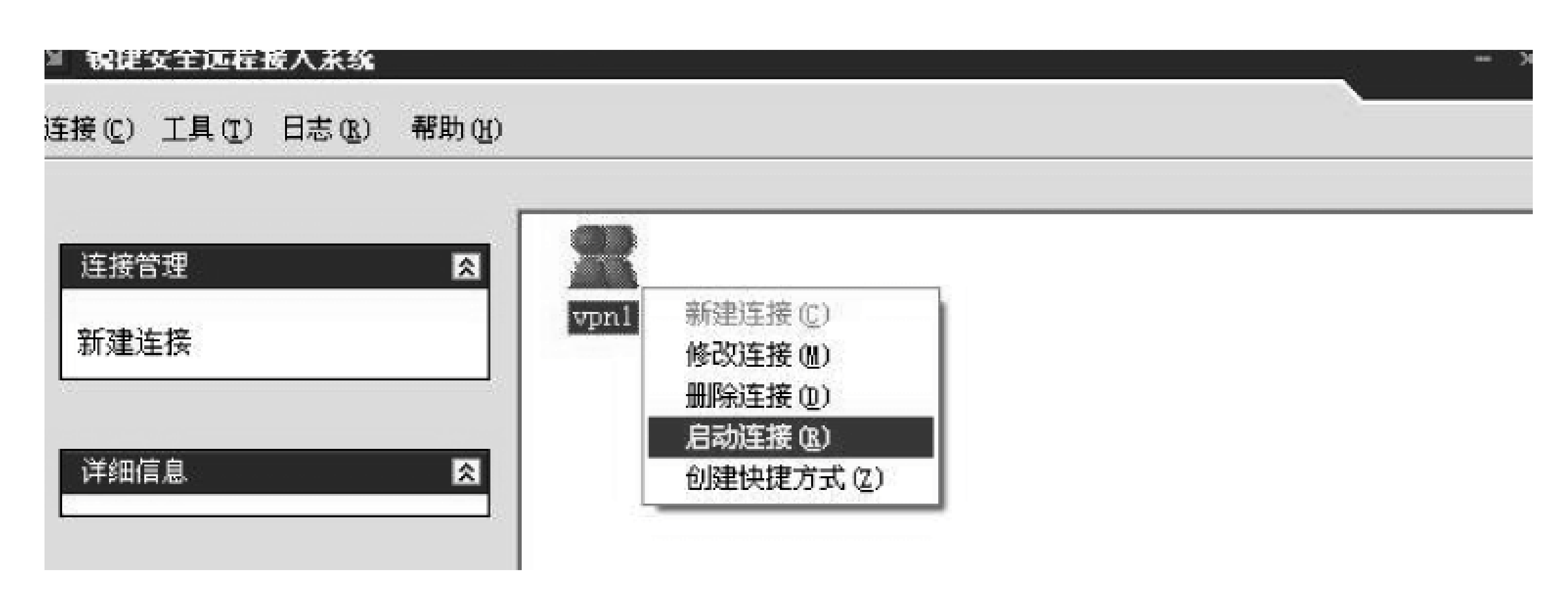


图 15.21 启动连接

输入用户名和密码，用户名为 test 和密码为 1234，用户是已在 VPN 上创建的用户，如图 15.22 所示。



图 15.22 输入用户名和密码

如果连接成功可以查看到如下信息，如图 15.23 所示。现在可以正常访问内网资源了。



图 15.23 VPN 连接成功信息

15.4 采用 USB-Key 的数字证书方式进行 VPN 通信

15.4.1 在远程用户管理中配置“认证参数”

界面如图 15.24 所示。



图 15.24 认证参数

15.4.2 证书管理系统 RG_CMS 的使用

证书管理系统的密码：admin，如图 15.25 所示。

添加新用户，CMS 为用户生成证书前必须先添加该用户，此处的用户类型可以是 VPN 网关，也可以是客户端用户（远程接入必须用这种用户）。这样系统才能对用户的证书进行管理和维护。

1. 添加客户端用户

在主菜单上选择“用户操作”→“添加新用户”或在管理视图区中的用户列表控件中单击右键，在弹出的菜单中选择“添加用户”，会弹出用户信息配置对话框，请输入相应的信息。如图 15.26 所示，用户信息配置对话框中各项输入栏中输入字符的内容及长度是有限制的，其中前 6 个（即国家、省/直辖市、城市/地区、组织、部门、用户）输入栏中不能填写以下字符 /\ * ：？<>｜"￥＃等，只能输入数字和英文，并且前 6 项输入字符总数相加不能超过 100 个。在用户信息对话框中的输入项说明：

国家：输入国家或者省份，输入字符长度只能为 2 个字符，如 cn。

省/直辖市：输入省或市的名称，如 bj。

城市/地区：输入城市或者地区，如 bj。



图 15.25　证书管理系统登录

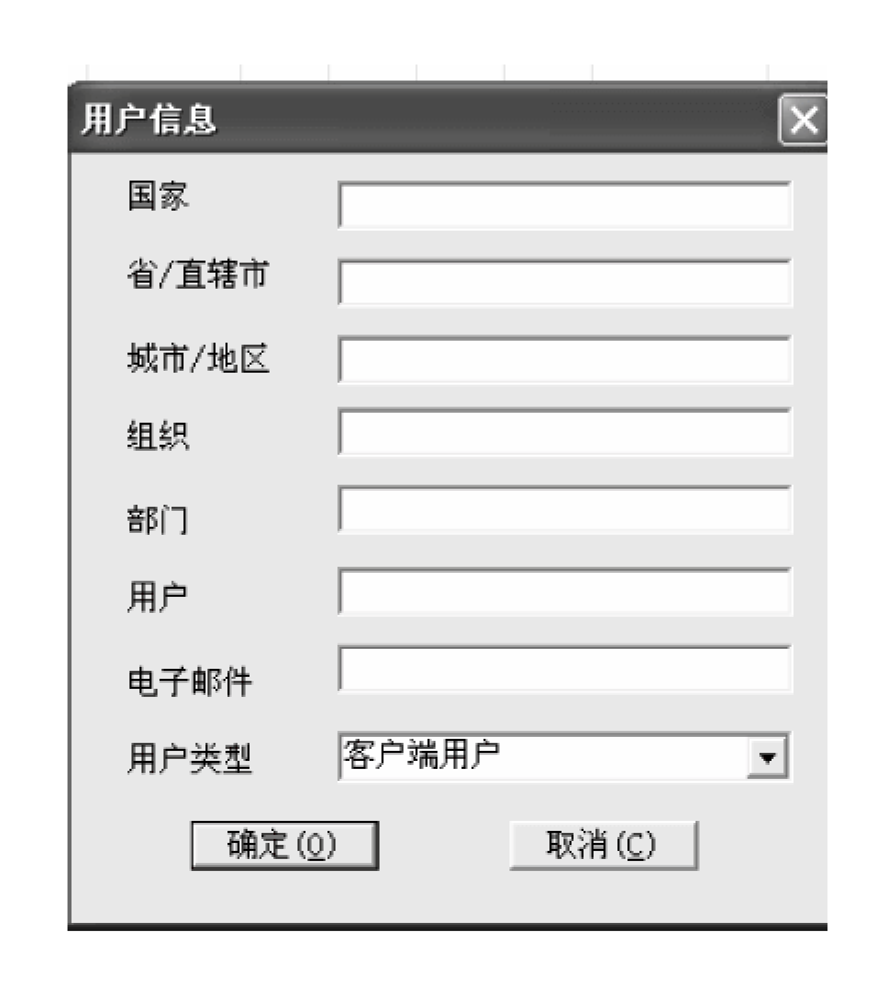


图 15.26　“用户信息”对话框

组织：输入组织名，如 security。

用户：输入用户的拼音或英文名，如 zhangsan、Jack，需要注意的是：在证书管理系统中，用户名必须唯一，不能重复，否则新添用户时将无法添加。

电子邮件：接收通知邮件的用户邮箱地址，输入一定要正确，否则用户将接收不到邮件通知，对该用户证书和私钥的远程分发工作将无法继续进行；如果不对证书和私钥进行远程分发，而是通过其他形式进行分发，此项可以填写虚拟的邮件地址。

用户类型：证书用户类型可为“客户端用户”和“网关用户”，其中客户端用户即安全远程接入系统客户端，网关用户即 VPN 网关用户，根据用户类型选择需生成的用户证书类型。请选择“客户端用户”。

上述信息输入完毕，请单击“确定”按钮，成功时将弹出成功操作提示框，在证书管理视图中，证书管理系统树控件显示新生成的证书节点信息，用户列表区中显示完整的用户证书信息，用户列表控件当前显示的是输入的用户信息。

2. 添加网关用户

与“添加安全远程接入系统用户”基本相同，区别是在选择用户类型时要选择“网关用户”。

3. 为用户生成证书

在用户列表控件中单选(或多选)要生成证书的用户，右击，在弹出的菜单中选择“生成证书”，如图 15.27 所示。

当然，也可以选择主菜单中的“证书操作”→“生成证书”，执行生成证书过程，系统会弹出等待状态条；生成证书后，系统会弹出操作成功提示框；管理员可以在信息窗口中对生成的证书和私钥进行察看。

4. 导出证书和私钥

执行导出证书及私钥操作前，要先选中一证书用户，并且已经成功执行过“生成证书”操作，否则此功能菜单为灰色不可用状态。

选择主菜单中的“证书操作”→“导出证书及私钥”(或在管理视图区中的用户列表控件中选中用户后单击右键，在弹出的菜单中选择“导出证书及私钥”)，弹出浏览存放路径对话框，如图 15.28 所示。通过单击“浏览”按钮，选择证书导出后存放的位置。



图 15.27 生成证书



图 15.28 导出证书和私钥

15.4.3 RG-SRA 程序的使用

在 PC 上运行 RG-SRA 程序，开始建立 VPN 隧道，如图 15.29 所示，单击“新建连接”按钮。



图 15.29 建立 VPN 隧道

填写如图 15.30 所示的基本信息，认证方式选择“数字证书认证”。



图 15.30　填写基本信息

按鼠标右键，启动连接，如图 15.31 所示。



图 15.31　启动连接

在弹出的窗口中单击“获取证书”按钮，如图 15.32 所示。

在弹出的对话框中选择“从 USB_Key 中读取”，如图 15.33 所示。



图 15.32　选择获取证书



图 15.33　从 USB_Key 中读取

在弹出的对话框中输入 pin 码：ruijie，如图 15.34 所示。

如果连接成功可以查看到如图 15.35 所示的信息，现在可以正常访问内网资源了。



图 15.34　输入 ruijie



图 15.35　配置信息

实验思考题

1. 证书登录和 USB-Key 登录各有什么特点？
2. 直接传输的数据包和 VPN 传输的数据包有何不同？
3. VPN 的配置主要配置什么参数？
4. 如果想允许某主机作为管理主机，该如何配置？
5. 如果想允许 VPN 用户访问某网段，又该如何配置？
6. 如何添加新的认证用户？
7. 如何在客户端进行登录？

参 考 文 献

1 戴英侠等.系统安全与入侵检测[M].北京:清华大学出版社,2002.

2 王艳柏,谭璐. 网络安全的探讨[J]. 长春大学学报,2005,(02).

3 2006 年第 38 届世界电信日:推进全球网络安全[J]. 中国教育网络,2006,(06).

4 王亚原. 企业网络安全问题及对策[J]. 太原师范学院学报(自然科学版),2005,(01).

5 (美)拉菲著. 思科网络技术学院教程 网络安全(第一、二学期)[M].北京:人民邮电出版社,2007.

6 李华清. 网络安全威胁和网络监管的现状、问题及对策研究[D]. 上海:上海交通大学,2007.

7 蒋义军. 基于 PKI 的信息安全技术研究与开发[D]. 电子科技大学,2003.

8 斯托林斯(Stallings,W.)著.密码编码学与网络安全——原理与实践.第四版[M].孟庆树等译.北京:电子工业出版社,2006.

9 张敏波. 网络安全实战详解[M]. 北京:电子工业出版社,2008.

10 (美)马里克(Malik,S.)著.网络安全原理与实践[M]. 王宝生,朱培栋,白建军 译. 北京:人民邮电出版社,2008.

11 思科系统(中国)网络技术有限公司 编著. 下一代网络安全[M]. 北京:北京邮电学院出版社,2006.

12 龙冬阳. 网络安全技术及应用[M]. 广州:华南理工大学出版社,2006.02

13 徐国爱,张森,彭俊好. 网络安全.第 2 版[M].北京:北京邮电学院出版社,2007.

14 葛秀慧,田浩,金素梅. 计算机网络安全管理.第 2 版[M].北京:清华大学出版社,2008.

15 袁津生,齐建东,曹佳. 计算机网络安全基础.第三版[M].北京:人民邮电出版社,2008.

16 顾巧论. 计算机网络安全——大学本科计算机专业应用型规划教材[M].北京:清华大学出版社,2004.

17 安淑梅. VPN 实验指导书:锐捷网络大学. 锐捷公司,2007.

18 胡建伟. 网络安全与保密[M]. 西安:西安电子科技大学出版社,2003.

附录 A　腾飞科技集团公司（公司名为虚构）网络信息系统的安全方案建议书

腾飞科技集团网络信息系统的安全

方案建议书

深度网络安全公司（公司名为虚构）
地址：上海市
技术支持热线：021-88998899
公司主页：www.8899.com.cn
电话：021-88998899　　传真：021-82828282

A1 需求分析

A1.1 网络安全集中管理的业务目标

为提升集团的创新能力，满足集团跨越式发展要求，增强集团整体竞争力，需要大力加强信息化建设，以便理顺和优化集团管控模式和业务流程，提高整个集团信息化应用水平。

信息化建设包括网络、服务器、存储及应用等子系统。而网络安全是顺利实现信息化建设的重要组成部分，规划和实行网络中心的网络安全建设便成为信息化建设中相当重要的环节。

通过网络安全技术建设和管理规划，建立完善的集团网络安全体系，包括网络安全政策、标准、流程、操作手册和管理制度，以及专题安全设计，以满足信息化建设的安全保障要求。保护集团信息资产不受诸多威胁的侵犯，确保业务的连续性，将业务损失和风险降低到最小程度。

A1.2 网络安全现状及需求说明

集团经过一期和二期网络建设和改造，初步建成了覆盖 40 家企业的集团企业网。其中骨干网有 4 个一级节点，10 个二级节点，25 个三级节点。

在上面的网络建设的基础上，各节点也独立建设了一些安全措施，例如在连接 Internet 的外网安装防火墙，在内网建设防病毒系统，进行域的建设等，同时也建立一些相应的管理制度。但是，这些措施和制度没有形成完善的体系，也没有一个机构进行全局的、整体的规划和设计。我们知道，在网络安全领域有一个“木桶效应”：就像木桶装水一样，木桶装水的多少是取决最短的一块木板的，信息系统的整体安全性也是取决最短的一块木板的。随着集团的网络的扩充，分支机构逐渐地增加，如果没有一套完善的安全标准，分支机构各自为战，每个机构对自身安全的考虑角度不同，安全系统的实施的效果也就不同。也就是说，在某个分支机构，如果有某个方面存在安全疏忽就可能成为整个系统的后门。

鉴于此，在本次网络中心网络规划的同时，准备建设集中的网络安全管理体系，该体系涉及的分支机构包括网络中心、生产地址、生产基地、开发中心、物资采购中心、集体总部。我们需要从整体安全的角度出发，建立一个涵盖这些分支机构的、完善的、统一的、可实施的网络安全体系。

A1.3 需求分析及设计思路

A1.3.1 需求分析

在充分了解集团的网络安全需求情况下，根据我们在企业网络安全建设方面的经验，建议分层次逐步建设集团的网络安全体系，从以下三个方面考虑本次网络安全系统的建设。

（1）从“网络安全中心”出发，实现分布式的网络安全布局，集中式的网络安全管理：

- 在准备新建的网络中心建立集团网络安全中心（以下简称网络安全中心）；
- 建立集团整体的网络安全体系；
- 在“网络安全中心”建立网络安全管理平台；

- 在分支机构,包括“网络中心”、“生产基地”、“物资采购中心”、“开发中心”和区域总部建立分支机构安全体系;
- “网络安全中心”制定统一的网络安全制度和规范;
- “网络安全中心”进行全局的考虑并对各分支机构进行网络安全集中管理;
- 各分支机构严格按照统一的网络安全制度和规范,对本部的网络安全体系实行相对独立的管理。

(2) 从“边界”及“互联”出发,实现中心与分支机构之间的“边界”的网络安全建设和管理:

- 在网络中心和各分支的网络边界处部署安全防护系统,保证中心和分支机构信息系统不受外界侵入;
- 在网络中心和各分支的网络传输链路上部署信息加密系统,保证中心和分支之间传输的数据的安全。

(3) 从“分支机构”出发,实现各分支机构内部网络安全的建设和管理:

- 在各分支机构建立相同的网络安全体系,以满足各分支机构自身的网络安全需求;
- 分支机构可对本部的网络安全体系进行管理;
- 网络中心的网络安全管理中心又可集中管理各分支的网络安全体系。

总的来说,对网络安全中心而言,它具有集中管理各分支机构网络安全体系的能力;对互联的边界而言,它具有防止外来入侵和传输加密的功能,同时又可被中心集中管理;对分支机构而言,它具有自己的网络安全体系,并可对其进行管理。

A1.3.2 设计思路

根据以上需求分析,我们结合集团的业务特性,设计思路如下:

(1) “中心”。网络安全管理中心(位于网络中心)的建设,包括:

- 建设统一的企业安全管理平台;
- 建设统一的 Windows 域,并规划各自的信任关系;
- 建设统一的内网安全及管理系统;
- 建设统一的防病毒管理系统;
- 建设统一的身份认证系统;
- 建设统一的文档保护及安全审计系统;
- 网络安全制度和规范的制定,包括面向中心和面向分支。

(2) “边界”及“互联”。各分支与网络中心互联的网络边界及链路安全建设,包括:

- 防火墙;
- 异常流量分析;
- 数据传输加密(VPN 或者 IP 加密机);
- 入侵检测及防护。

(3) “分支机构”。网络中心及各分支网络安全系统的建设,包括:

- 分支机构子域的建设和管理;
- 桌面防病毒;
- 内网安全及管理系统;
- 身份认证系统;

- 文档保护及安全审计系统；
- 防病毒网关(主要是指与 Internet 互联的外网)；
- 网络安全制度及规范的贯彻实施。

下面根据以上设计思路，对集团的安全需求进行初步的方案设计。

A2　总体方案设计

A2.1　方案综述

整个网络安全系统从物理上划分为 6 个部分，即网络中心、北京总部、两个生产基地、物资采购中心和开发中心。而从逻辑上则划分成一个网络安全中心和 6 个独立的子系统，其中在网络中心的安全机构同时扮演网络安全中心和网络中心子系统两个角色，北京总部、两个生产基地、物资采购中心和开发中心都作为子系统。

网络安全中心作为所有子系统的集合地，负责对 6 个子系统进行集中管理。

每个子系统是一个独立的安全区域，在严格遵守集团公司的网络安全制度和规范的前提下，每个安全区域有一套相对独立的网络安全系统，这些相对独立的系统能够被网络安全中心所管理。同时，在每个安全区域边界都进行有效的安全控制，防止安全事件扩散至其他安全区域，将事件控制在最小的范围内。

在以上的逻辑划分基础上，进行以下网络安全系统设计。

A2.2　网络安全中心设计

网络安全中心设计即集团网络安全管理体系的建设如下：

(1) Windows 域的建设。使用微软的活动目录，对网络进行域的划分。在网络中心建立根域，集中管理企业的资源。针对不同的分支建立各自的子域，并根据实际情况建立子域和根域、子域和子域之间的信任关系。

(2) 防病毒中心建设。使用企业版防病毒系统的分级管理功能，对网络进行管理单元划分。在信息中心建立一级防病毒服务器，负责所有二级防病毒服务器的统一管理。在不同的分支建立各自的二级防病毒服务器，负责本部的防病毒客户端管理。

(3) 内网安全及管理中心建设。使用内网安全及管理系统的分级管理功能，对网络进行管理单元划分。在信息中心建立内网安全及管理中心，负责所有分支内网安全及管理系统的统一管理。在不同分支建立各自的内网安全及防护系统，负责本部内网安全及管理系统的运维。

(4) 身份认证中心建设。在信息中心建立统一的身份认证系统，负责对各分支用户的身份进行管理，确保用户的身份安全，防止身份账号泄露带来的安全事件发生。

(5) 文件保护及安全审计中心建设。在信息中心建立统一的文件保护及安全审计系统，负责对各分支关键文件资源的保护，并对关键文件资源的访问进行详细的安全审计。

(6) 建立网络安全中心的企业安全管理平台。对所有的安全事件进行汇总分析，提供整个网络中网络安全的运行报告，并给出一个全局的安全事件分析，协助管理员对分散的安全事件点进行安全防护。

(7) 制定中心和分支相应的安全管理规范和规章制度。

(8) 充分利用服务商提供的安全服务对网络进行安全评估,对员工进行安全培训。在发生安全事件时,由服务商协助解决安全事件。随着网络安全的发展进一步完善网络中心网络的安全体系,同时又有坚固的安全服务后盾。

A2.3 边界及互联安全设计

边界及互联安全设计即网络中心与各分支机构互联的网络边界及链路安全的建设如下:

(1) 在与 Internet 连接的网络边界处部署防毒墙,对进入企业的数据包进行病毒扫描,控制外来访问,确保企业网络的安全性。

(2) 在网络中心与北京总部、各生产基地、物资采购中心及开发中心网络连接边界处部署防火墙,控制访问,增强数据访问的安全性。

(3) 使用防火墙集成的入侵检测及防护功能对所有进入信息中心的数据进行分析,识别非正常访问,并加以阻止。

(4) 在网络中心与北京总部、各生产基地、物资采购中心及开发中心之间,利用电信专线,结合防火墙 VPN 功能或者 IP 加密机,对数据传输进行加密,增强数据在传输过程中的安全性。

(5) 在网络中心及各分支网络边界部署"异常"流量分析系统,对所有进出的数据进行分析,对异常流量进行报警,协助管理员阻止异常流量进入企业内网。

A2.4 分支机构网络安全设计

分支机构网络安全设计即网络中心及各分支网络安全系统的建设,包括如下一些内容:

(1) 子域的建设。针对子域中不同部门和不同的用户设定不同的工作组,定制各自的策略和权限,有效地对资源、资源的访问以及员工的使用进行管理。

(2) 二级防病毒系统建设。在各分支建立二级防病毒服务器,在所有客户机部署桌面防病毒,负责本机的病毒防护。通过二级防病毒系统对本部的防病毒客户端进行管理,例如强制客户端升级病毒库,强制客户端开启防病毒软件等,以达到更好地防病毒效果。同时,防病毒二级服务器将本部防病毒运维状况汇总到一级服务器。

(3) 分支内网安全及管理系统建设。管理方面实现资产管理、远程协助、结合 Windows 域完成操作系统或补丁的分发等功能,对客户机操作系统的安全性和计算机所安装的软件进行有效地控制,对终端客户机进行远程协助等。安全方面实现外设控制,非法外联及非法接入,对客户机光驱、软驱、USB 移动存储设备进行有效地控制,防止员工利用这些移动存储设备泄漏公司机密;对员工计算机的网络连接进行有效控制,防止员工利用电话拨号等手段与外界进行信息通信;对外来人员自带计算机非法接入贵公司网络进行有效控制,防止外来人员的非法入侵。信息中心则可以通过中心管理平台了解甚至管理各分支内网安全及管理系统。

(4) 文件保护及安全审计系统建设。通过该系统,对重要的文件进行访问控制细化和审计,更大程度地保证公司文件的安全性,防止内部人员泄露公司机密,并且在发生泄漏事件后可以根据审计日志协助调查。

(5) 身份认证系统建设。对于权限较大的用户,我们建议采用强身份认证,以防止这些用户的账号被窃造成企业的损失。

(6) 在网络中心初期建设时可以建立统一的账号管理系统,实现将来多应用系统的账号整合。

A3 网络安全中心的建设

A3.1 Windows 域建设

Windows 域的建设使用微软的活动目录,对网络进行域的划分。在信息中心建立根域,集中管理企业的资源。针对不同的分支建立各自的子域,并根据实际情况建立子域和根域、子域和子域之间的信任关系。

另外,域建设是内网管理的基础平台,许多内网管理系统都是基于域工作的,因此域的建设相当重要。我们建议把 Windows 域作为最基本的安全措施在整个集团信息系统中实施,通过域的实施,可以提高整个系统的安全性。

根据网络中心的实际情况进行域的设计:

(1) 在网络中心,部署主备两台根域控服务器,对整个集团的 Windows 资源进行管理,且主用备用进行热备份,防止单点故障。

(2) 在各分支机构,部署主备两台子域控服务器,对本部的 Windows 资源进行管理,且主用备用进行热备份,防止单点故障。

(3) 根据各分支的各部门,建立不同的工作组,在工作组中,建立不同的用户,确保每人一个账号,针对账号设定不同的策略和权限。

A3.2 桌面防病毒部署

A3.2.1 方案设计

建议在网络安全中心建立企业级防病毒系统,以达到集中管理的目的:

(1) 在网络安全中心部署防病毒控制中心,即一级防病毒服务器。

(2) 在各分支部署二级防病毒服务器。

(3) 一级服务器负责病毒定义代码的更新,从 Internet 更新,如果服务器不能直接连接 Internet,则可由管理员下载后手动更新。

(4) 一级服务器更新完成后,将新的病毒定义代码推送到各二级服务器,二级服务器接收到后进行更新。

同样策略的分发也是由上至下,由防病毒控制中心制定防病毒策略,通过一级服务器分发到二级服务器,再由二级服务器分发到客户端;如果分支机构现有防病毒系统与将要采用的企业防病毒系统不同,可以逐步过渡到统一的防病毒系统来。

经过这样的防病毒部署,整个集团网络安全系统就具有了一个可统一管理的防病毒系统,大大增强了企业对病毒的抵抗力,提高了员工利用计算机工作的效率。同时也方便了管理员对客户机的管理,提高了管理员的工作效率。

A3.2.2 产品选型

根据网络中心的实际情况，结合目前防病毒软件厂商的特点，推荐使用 Symantec Antivirus 企业版防病毒软件。其特性如下：

(1) 从一个管理控制台提供高级的、企业范围的病毒防护和监视。

(2) 扩展威胁检测和威胁分类功能可识别不受欢迎的应用程序，如间谍软件和广告软件。

(3) 威胁跟踪器可识别通过开放式文件共享进行传播的混合型威胁攻击的来源(如 Nimda)。

(4) 出站电子邮件蠕虫启发式技术可防止客户端系统通过电子邮件传播蠕虫病毒。

(5) 可以对通过 POP3 邮件客户端(如 Outlook、Eudora 和 Netscape Mail)传输的传入电子邮件进行互联网电子邮件附件扫描。

(6) Symantec VPN Sentry 能够确保系统在访问企业网络资源前完全遵从企业策略。

(7) 存储和转发警报功能可确保未连接到网络的计算机在重新连接到网络后存储事件数据，并将事件数据转发给管理员。

(8) 内存中扫描功能可检测威胁，并在威胁造成破坏之前终止内存中的可疑进程。

(9) 集中化的网络审核功能帮助识别未受保护的节点以及受到 Symantec Antivirus Corporate Edition 的保护或选择了第三方安全产品的节点。

(10) 由世界领先的互联网安全研究和支持组织——赛门铁克安全响应中心提供支持。

A3.3 内网安全及管理

A3.3.1 方案设计

(1) 在网络安全中心部署中心核心服务器及内网管理控制中心。

(2) 在各分支部署分支核心服务器及分支管理控制中心。

(3) 信息中心可以通过内网管理控制中心对本部和各分支的分支核心服务器进行管理。

(4) 各分支可以通过分支控制中心对本部的核心服务器及客户端进行管理。

A3.3.2 产品选型

根据方案设计的内容，推荐 LANDesk 管理套件和 e-Cop 网络巡警，由两个产品合作实现内网安全和管理。

1) LANDesk 管理套件的特性

(1) 保持最新的安全补丁和病毒更新，能够高效地自动进行漏洞评估，修补以及即时的补丁管理(该组件需单独购买)。

(2) 高效的安装和维护桌面软件，包括 LANDesk 程序生成安装包、多文件 MSI 安装包、独立软件安装包、WISE 安装包等。

(3) 减少软件许可证的费用以及响应审计的要求，可以轻松地了解当前网络中应用软件的使用数量，可以知道当前软件的使用趋势，也可以限制许可证的使用数量，确保公司的软件使用符合许可。

(4) 降低支持中心费用。

(5) 管理物理设备、合同以及财务资产，能够收集所有的计算机软硬件资源，如所管辖客户端的计算机的 BIOS 参数内容、CPU 类型、内存数量、系统信息、操作系统版本、已安装的软件等。

(6) 向新操作系统迁移用户和配置信息，自动化的配置文件迁移保存用户、系统和应用程序设置并且在迁移完成后自动恢复配置。

(7) 实施计算机外设的控制，例如关闭 USB、MODEM、并口、串口等，防止非常外联，非法复制文件。

(8) 可以帮助远程的客户端进行异地操作和检查系统问题，充分发挥、共享服务器端的技术优势。

2) e-Cop 网络巡警主要实现对外来人员接入内网的控制的特性

(1) 提供全浏览器、中文化的用户操作界面，使用和操作非常简单、直截了当。

(2) 基于 Web 的网络管理系统，可以同时支持多人在不同的地点访问管理网络。

(3) e-Cop 自身带有用户身份认证和授权管理系统，保证其自身的安全。

(4) 实时扫描获取与分析在线计算机的 IP 地址信息。

(5) IP 地址、MAC 地址的合法性判定。

(6) 支持 IP-MAC 绑定、特权 MAC 地址和 DHCP MAC 地址三种合法性管理方式。

(7) 警告和阻断使用非法 IP 地址的计算机。

(8) 统计分析非法 IP 地址使用的历史情况。

(9) 支持主动探测和被动侦听等多种扫描方式。

(10) 通过在各网段部署的 IP 地址管理代理服务器收集本网段 IP 地址信息，并汇总到管理服务器上进行全网集中管理。

A3.4 文件保护及安全审计

A3.4.1 方案设计

(1) 在网络中心和各分支部署文档保护及安全审计系统。

(2) 网络安全中心和各分支的管理员通过控制台管理本部的文档保护及安全审计系统。

(3) 网络安全中心的管理员可以通过 Web 浏览器浏览本部及各分支的安全审计日志，以了解各分支文件保护及安全审计系统的运行状况。

(4) 客户端需要添加解密客户端软件，用户使用浏览器下载文件后利用解密客户端软件进行操作。

A3.4.2 产品选型

这一类产品国内研发较多，可选范围也比较大，推荐前沿科技文档安全管理系统(eDocGuard)。其产品特性如下：

(1) 核心加密技术，128-bit Encryption，X. 509 certificates，PKI。

(2) Server 跨平台支持，J2EE Platform / Windows。

(3) 支持文件格式 Microsoft Office、PDF、AutoCAD、TXT、JPG、BMP 等。

(4) 支持 LDAP V3.0(DOMINO、AD)。

(5) 可控制阅读、复制、打印、拷贝、还原等权限和到期日。

(6) 具有强审计功能,可以做到 A 用户 B 时间在 C 计算机对 D 文档做了 F 操作的审计。

(7) 可以做到离线认证,即用户离开公司环境后仍可打开文档,但仅限于本机打开,复制后文件失效。

A3.5 企业数字身份管理系统

A3.5.1 方案设计

建立基于公钥技术的安全平台(含证书认证中心、密钥管理中心、审核注册中心、密码与认证服务系统等),对各类用户、设备的接入进行强认证,并在此基础上提供授权服务(身份验证、权限管理及访问控制、数据安全传输、数据安全存储、数字签名、审计和统计、时间戳服务、网页内容的防篡改等),从而实现对业务及数据的安全管理。

数字证书的格式一般采用 X.509 国际标准。目前,数字证书主要分为安全电子邮件证书、个人和企业身份证书、服务器证书以及代码签名证书等几种类型证书。

在网络安全中心部署企业数字身份管理系统,所有证书都由该系统根据使用者的身份进行派发。在需要保护的服务器以及个人主机上安装安全认证代理客户端软件。

派发的数字证书采用 PKI(Public Key Infrastructure,公开密钥基础架构)技术,利用一对互相匹配的密钥进行加密和解密。每个用户自己设定一把特定的仅为本人所知的私有密钥(私钥),用它进行解密和签名;同时设定一把公共密钥(公钥),由本人公开,为一组用户所共享,用于加密和验证签名。当发送一份保密文件时,发送方使用接收方的公钥对数据加密,而接收方则使用自己的私钥解密,通过数字的手段保证加解密过程是一个不可逆过程,即只有用私有密钥才能解密,这样保证网络安全无误地到达目的地。用户也可以采用自己的私钥对发送信息加以处理,形成数字签名。由于私钥为本人所独有,这样可以确定发送者的身份,防止发送者对发送信息的抵赖性。接收方通过验证签名还可以判断信息是否被篡改过。在公开密钥基础架构技术中,最常用的一种算法是 RSA 算法,其数学原理是将一个大数分解成两个质数的乘积,加密和解密用的是两个不同的密钥。即使已知明文、密文和加密密钥(公开密钥),想要推导出解密密钥(私密密钥),在计算上是不可能的。按现在的计算机技术水平,要破解目前采用的 1024 位 RSA 密钥,一台计算机需要上千年的计算时间。即使是调集全世界所有的计算机,也需要一年半的时间才能够破解。

A3.5.2 产品选型

上海市数字证书认证中心有限公司的 UniTrust® DIDMSTM-Ⅰ型是 SHECA 在实际运作过程中,根据用户需求开发的一套企业级的 PKI 解决方案套件。它通过提供身份认证等服务,使用户能以最少的投资建立起一个可控、方便的信息化安全管理系统。

DIDMSTM 是一台软硬一体机设备,DIDMSTM 产品支持各类国际标准并采用国家密码委员会认可的加密算法模块,能够存储长达 7 年的证书量,可签发 1～10 000 张证书。它同时支持 UniTrust® 的 SafeEngine 和证书管理器,以进行应用开发。

系统采用一级管理模式代替 CA-RA 结构,应用动态口令技术确保密钥的在线安全使用。此外,简洁美观的 Web 操作界面,简单易用。DIDMSTM 为软硬一体机,能够充分发挥硬件特性,便于管理和维护,并减少人为干预。

DIDMSTM 可与以下软件协同工作：

- 客户端应用程序　Netscape Navigator，Netscape Communication，Microsoft Internet Exploer，UniTrust® SafeEngine，UniTrust®证书管理器。
- 各种 Web 服务器　Microsoft IIS WebServer，Netscape Enterprise，Apache，Java WebServer，Domino 等。
- 遵从 X.509 和 PKCS 的所有 PKI 应用程序。

充分满足或支持国际标准：X.509v1、X.509v2、X.509v3、CRL、OCSP、TimeStamp、PKCS1、PKCS8、PKCS7、PKCS10、ASN1、MIME、SSL、SMIME、LDAP。

采用国家密码委员会认可的加密算法：RSA、SDBI、SHA1、MD5、MD2。

A3.6　强身份认证

对于权限较大的用户以及网络管理的用户，建议采用强身份认证，以防止这些用户的账号被窃造成企业的损失。

建议结合域账号，为这些权限较大的用户增加动态令牌的强身份认证系统，增强对这些用户的账号保护，确保使用这些账号的人的合法身份。

一般意义上的身份认证是指使用者在登录某系统或应用时输入用户名和密码，系统或应用确认用户名和密码正确后，释放权限给使用者。但这样的认证方式始终存在漏洞，如果该用户名和密码被人窃取，那么系统或软件就无法识别这个使用的人是合法拥有者，还是窃取者。因此，确认使用者合法身份成了身份认证需要解决的问题。

动态令牌产品是基于强密码的身份认证系统，用户在进行系统身份认证时需要输入用户名、静态 PIN 码、动态密码三个要素，才能正常登录。而动态密码存放在一块包含石英钟和加密算法的令牌卡上，该密码每分钟变换一次，且只能使用一次。基于这样的认证方式，窃取者即使窃取了用户名和静态 PIN 码也无法登录系统。大大加强了对使用者的合法身份的保护。

目前业界比较成熟，且口碑非常好的产品 RSA Secure ID，能够与用户环境良好的结合，并且达到非常好的身份保护效果。

A3.7　企业安全管理平台

A3.7.1　方案设计

网络管理员要想达到更好的管理网络效果，进行日志分析是非常重要的。通过对日志的分析，可以做到追踪重要的事件以供审计、提供调查所需的资料、确定异常的事件和确认责任等。确定一些紧要的安全事件，加以规划、整合、分析、关联及做出，适当的追踪、调查及应对措施。

而如今众多的安全产品都具有自己的日志系统，各自为政，很难为管理员提供一个统一的安全事件分析。

通过企业安全管理平台，便可为企业提供一个统一的安全事件管理系统。此系统可以整合、划一、关联及分析多元系统日志，可以在一个平台上处理任何系统的日志。具有误报过滤、自动处理、攻击归类和预警功能。独立于安全设备厂家，支持加密安全通信，没有代理服务器，具有动态数据挖掘和分析功能，同时具有风险管理和应对措施功能。还有，它具有

追踪和报表功能。

A3.7.2 产品选型

推荐使用目前在安全管理方面表现较为突出的产品 e-Cop 公司的 Cyclops ESM 企业网络安全管理系统，该系统的特点如下：

(1) 具有跨平台、跨规格的安全事件推论引擎。

(2) 支持四种语言(含双字节)英汉(简/繁体)及日文。

(3) 含 8 种不同推论知识库和事件关联的技术，可沟通超过 50 种品牌的产品(ESM & NMS)。

(4) 可以整合、划一、关联及分析多元系统日志，在一个平台上处理任何系统的日志。

(5) 具有误报过滤、自动处理、攻击归类和预警功能。

(6) 独立于安全设备厂家，支持加密安全通信，没有代理服务器，具有动态数据挖掘和分析功能。

(7) 具有风险管理和应对措施功能。

(8) 具有追踪和报表功能。

(9) 支持众多主流厂商的产品。

A3.8 安全管理体系(管理制度)

对于一个完善的安全系统，必须具备相应的管理体系，只有在行政和技术上同时达到安全，才能实现真正的安全。因此，建议集团公司建立安全管理组织机构，并且制定相应的安全规章制度，以辅助整个安全系统的运行。

依据国家法律法规标准、国际标准和集团具体情况制定企业级的安全政策、标准和流程，为日常的安全管理、安全决策提供成文的、统一的安全指导，提高安全管理和决策水平。以下提供内容参考一部分：

A3.8.1 安全管理体系(管理制度)样例

网络中心的安全管理政策是指导如何对网络中心的资产，包括敏感性信息进行管理、保护和分配的规则和指示。网络中心不仅需要一个整体的安全政策，而且，在整体政策的框架内，根据风险评估的结果，需要制定更加具体的安全政策，明确规定具体的控制规则，如“清理桌面和清除屏幕方针”、“访问控制方针”等。

网络中心的网络安全总体政策需要阐明网络中心管理层对安全的承诺，提出网络中心管理网络安全的方法，并由管理层批准，采用适当的方式(安全意识宣传和培训)将政策传递给员工。网络中心的总体网络安全政策至少应包括以下内容：

(1) 网络安全的定义，总体目标、范围，安全对信息共享的重要性。

(2) 管理层意图、支持目标和网络安全原则的阐述。

(3) 安全政策的原则、标准的简要说明，以及依从具体要求对网络中心的重要性。

(4) 网络安全管理的一般和具体的责任定义，包括报告安全事故。

A3.8.2 总政策样例

1) 总体目标。网络安全就是通过防止和最小化安全事故的影响，保证网络中心业务持续性并最小化商业损失。

2）网络安全政策的内容如下：

（1）政策的目标是保护网络中心的信息资产，防止所有的威胁，无论是内部的还是外部的，有预谋的还是突发性的。

（2）网络中心最高管理者要批准网络安全政策。

（3）网络中心的安全政策要保证：信息应该防范未经授权的访问。

（4）确保信息的保密性。

（5）维护信息的完整性。

（6）应顺应法规和规章的要求。

（7）制定、维护和试验业务持续性计划。

（8）所有员工都要接受网络安全培训。

（9）对网络安全的所有破坏，包括实际存在的或可疑的，都要报告，对此网络安全管理员进行研究。

（10）现有的支持安全政策的程序，包括病毒控制、密码保护等。

（11）应满足信息和信息系统可用性的商业要求。

（12）网络安全管理者应该对维护政策负直接责任，并在政策实施过程中，提供建议和指导。

（13）所有的管理者对在他们工作区域执行的政策负有直接责任，并保证员工遵守政策。

（14）每一个员工的职责就是遵守政策。

3）为了确保安全政策的持续的适应性和有效性，网络中心要定期进行评审和评价，内容通常包括：

（1）政策的有效性，由记录在案的安全事件的性质、数量和影响来证明。

（2）技术变更的影响。当网络中心影响风险评估的基础发生变化时，应及时对政策进行评审，如重大网络安全事件发生、新的漏洞、网络中心组织结构或技术基础发生变更等。

A3.8.3 具体安全政策样例

除了总体政策，网络中心应根据其特定具体要求编制和执行具体的安全政策。在网络中心的环境中至少包含以下具体安全政策：

- 《机房安全管理规定》
- 《用户名、口令安全管理规定》
- 《电子邮件使用安全管理规定》
- 《系统变更管理规定》
- 《系统管理员角色分配和安全守则》
- 《远程维护安全管理规定》
- 《网络设备配制规范》
- 《防火墙配制规范》
- 《信息系统数据备份规范》
- 《病毒防治安全规范》
- 《应用安全管理规定》
- 《介质管理规定》

- 《第三方访问管理规定》
- 《桌面安全规定》
- 《应用拥有者规定》
- 《应用开发安全规定》
- 《计算机环境安全制度》
- 《数据和信息定级(归类)规定》
- 《紧急情况登录规定》
- 《数据加密规定》
- 《离线存储规定》
- 《打印和发布规定》
- 《生产文件变更制度》
- 《安全违规定级规定》
- 《声音系统安全规定》
- 《FAX、Modem 系统使用规定》

⋮

A3.8.4 安全管理流程样例

基于网络中心的安全政策或安全管理制度,网络中心的 IT 安全管理流程至少应包括以下内容:

- 安全突发事件/违例管理流程
- 安全变更管理流程
- 安全审计管理流程
- 安全补丁管理流程
- 安全备份流程
- 安全监控流程
- 安全风险评估流程
- 安全计划维护流程

A3.9 安全服务

A3.9.1 安全评估

安全评估服务可以充分揭示客户网络系统整体而全面的安全现状。可根据业界标准(BS7799/ISO17799)及操作惯例,分析客户现有的安全策略及控制过程,实施外部/内部安全扫描,在发掘出已知漏洞的情况下,向客户提供具体的应对措施及解决方案。在安全评估基础上,依据业界惯例来实施有针对性的系统安全加固服务。

在实施安全评估服务过程中,会采用多种符合标准的测试和操作工具,这些工具各具特色,每个工具单独来讲,都在某一方面或某一具体领域卓有成效,而将这些工具综合运用,恰好构成一个全面系统的漏洞扫描、测试的评估方案。

安全扫描

在网络安全体系的建设中,安全扫描工具花费低、效果好、见效快、与网络的运行相对独

立、安装运行简单，可以大规模减少安全管理员的手工劳动，有利于保持全网安全政策的统一和稳定，是进行风险分析的有力工具。安全扫描技术基本上也可分为基于主机的和基于网络的两种，前者主要关注软件所在主机上的风险与漏洞，而后者则是通过网络远程探测其他主机的安全风险与漏洞。

在本项目中，安全扫描主要是通过评估工具以本地扫描的方式对评估范围内的系统和网络进行安全扫描，从内网和外网两个角度来查找网络结构、网络设备、服务器主机、数据和用户账号/口令等安全对象目标存在的安全风险、漏洞和威胁。

从网络层次的角度来看，扫描项目涉及如下三个层面的安全问题。

（1）系统层安全：该层的安全问题来自网络运行的操作系统：UNIX 系列、Linux 系列、Windows 系列以及专用操作系统等。安全性问题表现在两方面：一是操作系统本身的不安全因素，主要包括身份认证、访问控制、系统漏洞等；二是操作系统的安全配置存在问题。

- 身份认证：通过 IPC＄进行口令猜测……
- 访问控制：注册表 HKEY_LOCAL_MACHINE 普通用户可写，远程主机允许匿名 FTP 登录，ftp 服务器存在匿名可写目录……
- 系统漏洞：System V 系统 Login 远程缓冲区溢出漏洞，Microsoft Windows Locator 服务远程缓冲区溢出漏洞……
- 安全配置问题：部分 SMB 用户存在薄弱口令，试图使用 rsh 登录进入远程系统……

（2）网络层安全：该层的安全问题主要指网络信息的安全性，包括网络层身份认证，网络资源的访问控制，数据传输的保密与完整性、远程接入、域名系统、路由系统的安全，入侵检测的手段等。

- 网络资源的访问控制：检测到无线访问点……
- 域名系统：ISC BIND SIG 资源记录无效过期时间拒绝服务攻击漏洞，Microsoft Windows NT DNS 拒绝服务攻击……
- 路由器：Cisco IOS Web 配置接口安全认证可被绕过，Nortel 交换机/路由器默认口令漏洞，华为网络设备没有设置口令……

（3）应用层安全：该层的安全考虑网络对用户提供服务所采用的应用软件和数据的安全性，包括数据库软件、Web 服务、电子邮件系统、域名系统、交换与路由系统、防火墙及应用网管系统、业务应用软件以及其他网络服务系统等。

- 数据库软件：Oracle tnslsnr 没有设置口令，Microsoft SQL Server 2000 Resolution 服务多个安全漏洞……
- Web 服务器：Apache Mod_SSL/Apache-SSL 远程缓冲区溢出漏洞，Microsoft IIS 5.0 printer ISAPI 远程缓冲区溢出，Sun ONE/iPlanet Web 服务程序分块编码传输漏洞……
- 电子邮件系统：Sendmail 头处理远程溢出漏洞，Microsoft Windows 2000 SMTP 服务认证错误漏洞……
- 防火墙及应用网管系统：Axent Raptor 防火墙拒绝服务漏洞……
- 其他网络服务系统：Wingate POP3 USER 命令远程溢出漏洞，Linux 系统 LPRng 远程格式化串漏洞……

为了确保扫描的可靠性和安全性，我们将根据网络系统业务情况，与客户一起确定扫描计划。计划主要包括扫描开始时间、扫描对象、预计结束时间、扫描项目、预期影响、需要对方提供的支持等。我们将与网络信息系统评估项目组一起协商具体需要扫描的项目。比如，为了防止对系统和网络的正常运行造成影响，我们将修改、配置一定的扫描、审计策略使资源消耗降低至最小，限制或不采用拒绝服务模块进行扫描。我们仅在可控环境下，对非重要服务的主机、设备进行拒绝服务扫描。对那些危险的模块和重要主机则主要采用手动检查的方式。另外，我们将在评估前将协助评估节点进行必要的系统备份，并检查本地的应急恢复计划是否合理。

在实际开始评估扫描时，我们会正式通知网络信息系统评估项目组成员。我们将按照预定计划，在规定时间内进行并完成评估工作。如遇到特殊情况（如设备问题、停电、网络中断等不可预知的状况）不能按时完成扫描计划或致使扫描无法正常进行时，由双方召开临时协调会协商予以解决。

手工检查

系统扫描是利用安全评估工具对绝大多数评估范围内的主机、网络设备等方面进行漏洞的扫描。但是，评估范围内的网络设备安全策略的弱点和部分主机的安全配置错误等并不能被扫描器全面发现，因此有必要对评估工具扫描范围之外的系统和设备进行手工检查。

系统的网络设备的安全性评估应主要考虑以下几个方面：

- 是否最优地划分了 VLAN 和不同的网段，保证了每个用户的最小权限原则；
- 内外网之间、重要的网段之间是否进行了必要的隔离措施；
- 路由器、交换机等网络设备的配置是否最优，是否配置了安全参数；
- 安全设备的接入方式是否正确，是否最大化地利用了其安全功能而又占系统资源最小，是否影响业务和系统的正常运行。

同时，许多安全设备如防火墙、入侵检测等设备也是人工评估的主要对象。因为这些安全系统的作用是为网络和应用系统提供必要的保护，其安全性也必然关系到网络和应用系统的安全性是否可用、可控和可信。目前还没有针对安全系统进行安全评估的系统和工具，只能通过手工的方式进行安全评估。

安全系统的安全评估内容主要包括：

- 安全系统是否配置最优，实现其最优功能和性能，保证网络系统的正常运行；
- 安全系统自身的保护机制是否实现；
- 安全系统的管理机制是否安全；
- 安全系统为网络提供的保护措施，且这些措施是否正常和正确；
- 安全系统是否定期升级或更新；
- 安全系统是否存在漏洞或后门。

渗透测试

渗透测试是指在获取用户授权后，通过真实模拟黑客使用的工具、分析方法来进行实际的漏洞发现和利用的安全测试方法。这种测试方法可以非常有效地发现最严重的安全漏洞，尤其是与全面的代码审计相比，其使用的时间更短，也更有效率。在测试过程中，用户可以选择渗透测试的强度，例如不允许测试人员对某些服务器或者应用进行测试或影响其正常运行。通过对某些重点服务器进行准确、全面的测试，可以发现系统最脆弱的环节，以便

对危害性严重的漏洞及时修补，以免后患。

技术人员进行渗透测试都是在业务应用空闲的时候，或者在搭建的系统测试环境下进行。另外，我们采用的测试工具和攻击手段都在可控范围内，并同时准备充分完善的系统恢复方案。

A3.9.2　安全加固

评估阶段结束之后，我们应该就加固阶段的具体事项与客户方进行协商，并为实施操作做好必要的准备。

根据安全评估的结果，并与客户方相关人员进行交流，复查相关文档资料，我们应该了解以下信息：

- 与目标服务器相关的所有业务、技术、应用程序需求。
- 所有针对目标服务器的安全策略及程序信息。
- 所有涉及备份、恢复的策略及程序。
- 所有当前的灾难恢复策略、程序及计划。

分析并掌握了客户的确切需求之后，我们将制定符合客户需求的安全加固计划，包括编写特定的脚本程序、准备相应的测试工具等。

A3.9.3　安全培训

管理人员涉及的安全培训为以下方面：

- 网络安全基础知识
- 什么是网络安全
- 网络安全的重要性
- 信息系统为什么会不安全
- 常见的安全隐患(物理环境不安全，弱口令，安全漏洞，不安全的工作习惯)
- 常用的一些安全防范措施
- 安全管理的重要性(让安全成为习惯)
- 安全现状和发展趋势分析
- 公司的安全规范、标准培训

普通员工涉及的安全培训为以下方面：

- 常用安全防范措施
- 网络安全基础知识
- 普通员工安全意识培训
- 公司的安全标准的培训
- 公司的安全操作流程的培训
- 公司的安全策略的培训
- 普通员工的安全职责培训

技术人员涉及的安全培训为以下方面：

- 黑客攻击技术分析
- 网络扫描技术培训
- 病毒及木马技术培训

- 缓冲区溢出技术培训
- 拒绝服务攻击技术(DOS 及 DDOS)培训
- 网络监听技术培训
- 系统管理员管理和操作流程培训
- 系统管理员管理职责培训
- 紧急事件响应流程培训

A3.9.4 紧急响应服务

在客户运行维护系统过程中,作为客户方的技术人员由于时间和精力的问题,常常对于这些紧急事件缺乏有效的处理,这样往往会对系统正常运转造成重大影响。我们提供的紧急安全响应服务,那么在服务期间,一旦客户系统发生紧急事件,我们就将派出专业安全工程师,到现场快速响应安全事件,解决安全问题,并根据出现的问题及时调整安全策略,帮助用户在以后的维护中正确解决问题。

A3.10 账号整合(可选)

随着信息系统应用的增加,账号也随之不断增多,有时一个员工需要记住近 10 个账号,这对于应用系统的使用带来了极大的不便。而账号整合的概念解决了这一大难题。利用账号整合将多应用系统的用户信息集合到一起,用户只需进行一次登录即完成了多个应用系统的认证过程,访问各个应用时无需在此认证。

账号整合系统通过将各应用系统的 LDAP 数据库整合到账号管理服务器上,用户认证经由该账号管理服务器进行认证,由此完成所有应用系统的登录。

而对于管理员,在对账号进行管理的过程中,也只需对账号管理服务器进行管理,不必再为一个员工在各应用系统的账号管理而分别对数个应用系统进行操作。

A4 网络安全中心与分支机构互联边界安全

A4.1 防火墙部署

A4.1.1 方案设计

我们根据集团的网络规划进行了防火墙的部署设计:

在网络中心企业网边界部署两台冗余高性能防火墙,连接两个生产基地、物资采购中心、开发中心和北京总部的广域网链路,对每个连接的分支分配一个安全域,所有经过防火墙的流量都将根据策略进行控制和筛选,只有符合防火墙规则的数据流才能正常到达目的地。通过访问的控制,很大程度上防止了非法的数据包进入网络中心,或者进入其他分支。并且防火墙能在企业网内部爆发病毒或蠕虫造成网络拥塞时,阻止病毒和蠕虫进入其他安全区域,防止某个区域的病毒爆发对其他区域造成影响;

网络中心两台冗余高性能防火墙定义为热冗余备份工作方式,当主用防火墙发生故障时,自动将所有会话切换到备用防火墙上,保证了网络的不间断性;

在两个生产基地、物资采购中心、开发中心和北京总部的广域网边界各部署两台中等性能的防火墙,同样采用热冗余的方式。对来自网络中心和其他分支的数据流进行控制筛选,

保证了本分支的网络安全性。如有必要也可以通过策略控制本分支到网络中心和其他分支的数据进行控制筛选；

如果希望对通过网络中心和各分支之间传输的数据进行加密，则可以使用防火墙的VPN加密功能来实现，即可以利用DDN线路配合防火墙VPN功能来实现，在网络中心和各分支之间建立VPN加密隧道，其传输的数据都经过168位加密(3DES)。

A4.1.2 产品选型

根据以上方案设计，我们推荐以下相关产品供用户选择。

北京总部、两大生产基地、物资采购中心和开发中心的边界防火墙，可以选择性能相对中等的防火墙，如Netscreen-204防火墙，其特性如下：

- 4个10/100M接口
- 400M防火墙吞吐量，200M 3DES吞吐量
- 最大会话数128 000
- 最大VPN隧道数1000，最大策略数4000条
- 拒绝服务攻击防护功能，可抵御30多种不同的内外部攻击
- 通过图形Web UI、CLI或Netscreen-Security Manager集中管理系统进行管理
- 基于策略的管理，用于进行集中的端到端生命周期管理

而对于网络中心的高性能防火墙，我们推荐Netscreen-ISG 1000防火墙，其产品特性如下：

- 4个固定的10/100/1000和最多4个Mini GBIC(SX或LX)，或最多8个10/100/1000，或最多20个10/100
- 吞吐量为1G防火墙，1G 3DES VPN
- 最大会话数250 000
- 最大策略条数10 000
- 最多VPN隧道数2000
- 最大安全域数默认为26个，可选为40个
- 高可靠性支持主用/备用、主用/主用、主用/主用，全网状
- 透明模式，允许设备作为第2层IP安全网桥运行，提供防火墙、VPN和DoS防护功能，但只需对现有网络进行最少的改变
- 集成IDP
- 基于策略的管理，用于进行集中的端到端生命周期管理
- 通过图形Web UI、CLI或Netscreen-Security Manager集中管理系统进行管理
- 支持SNMP，可被网管软件管理

A4.2 入侵检测及防护部署

A4.2.1 方案设计

入侵检测及防护功能集成在防火墙上，这样减少了网络中的串联设备，同时排出了由于串联过多设备造成的网络瓶颈。

基于网络的入侵检测及防护，在网络枢纽处，部署网络入侵检测系统，网络入侵检测系

统将从网络传输数据包的分析中判断一切网络行为是否合法，如果发现可疑的网络行为，则网络入侵检测系统会报警，并提示管理员。

入侵检测可以通过路由、桥接和端口镜像三种方式工作。其中路由和桥接模式可以对入侵行为进行阻止，但必须串联在网络中。端口镜像模式只需并联在网络中，但只能对入侵行为进行检测和报警。

A4.2.2 产品选型

入侵检测保护系统，我们建议可以采用在边界防火墙中集成的 IDP 功能来实现如下一些功能：

（1）应用层保护：无与伦比的安全处理能力和网络分段特性，允许 ISG 系列产品防止蠕虫、特洛伊木马、间谍软件和恶意软件等现有和新出现的应用层威胁入侵关键的高速网络并在网络中蔓延。状态特征和协议异常检测等多种攻击检测机制，使 IDP 能够深入分析应用协议、上下文和状态，以便针对现有和新型威胁提供 Zero Day 防护。

（2）网络友好：为了简化网络部署，ISG 系列产品将 IDP 功能与 ScreenOS 无缝集成，并全面利用公认的联网特性，如动态路由，包括 OSPF、BGP 和 RIP；通过虚拟路由器实现的多个路由域；NAT/路由/透明部署选项；无缝的 ScreenOS 集成还允许跨越虚拟系统和安全区域部署 IDP 攻击防护功能，以防止攻击侵入网络或在整个网络中蔓延。

（3）基于策略的管理：使用 Netscreen-Security Manager 提供的细粒度的逐条规则灵活性，管理员可逐条规则、逐个协议的部署串联 IDP 或串联开发模式。基于角色的管理允许安全团队将管理权分配给适当人员，从而使一个团队只负责管理 IDP 组件，而让其他团队管理防火墙、VPN 或其他任务。Netscreen-Security Manager 的直观用户界面允许用户快速轻松地管理攻击和事故调查以及审核与报告工作，以确保遵从安全策略。

A4.3 流量分析部署

A4.3.1 方案设计

在网络中心边界部署流量分析系统；

在各分支边界部署流量分析探针，将获得的数据汇总到网络安全中心，进行数据分析；

在主干交换机上设置端口镜像，Monitor 主链路的交换机端口；

将流量分析系统连接至设置过端口镜像的交换机端口，以抓取数据；

利用流量分析系统，对所有进入网络中心的流量进行分析，并做出分析报告；

如果发现异常流量，如病毒爆发等，则触发报警；

网管人员在网络安全中心使用中心控制台，可以方便地连接到流量分析系统远程分析引擎，实现对企业全部网络的监控分析。

A4.3.2 产品选型

该流量分析软件，我们推荐目前性价比较高的 WildPackets 公司的 OmniPeek 软件，其产品特性如下：

- 提供全网系统的实时故障诊断：包括网络、计算机及应用；
- 包含了与现今网络关联非常紧密的强大的分析工具；
- 非常直观，而且易于使用；

- 灵活的架构,对于新的应用非常易于扩展与升级;
- 可保护与优化网络;
- 基于信息流的专家分析系统和应用分析;
- 交互式节点图;
- 完整的七层协议解码;
- 应用响应时间(ART)分析;
- 安全功能;
- 监控与报表;
- RMON 分布式分析。

A5 分支机构网络安全建设

A5.1 Windows 域建设

在各分支,部署主备两台子域控服务器,对本部的 Windows 资源进行管理,且主用备用进行热备份,防止单点故障;

根据各分支的各部门,建立不同的工作组,对工作组设定各自的策略和权限;

在工作组中,建立不同的用户,确保每人一个账号,针对账号设定不同的策略和权限;

将整个网络中心的客户端加入域,接受域管理,并为软件和补丁分发奠定基础;

对用户的口令进行强化,强制客户端使用高强度密码,防止用户密码的泄漏,造成不必要的损失;

限制一些客户机的软件安装权限,确保工作用机只安装与工作有关的软件;

对一些与域结合的应用,如文件服务器等,还可以通过域完成单点登录的效果。

A5.2 桌面防病毒部署

在各分支部署二级防病毒服务器;

在所有客户端安装防病毒客户端软件,并接受防病毒控制中心的管理;

各分支的客户端病毒定义升级则是由二级防病毒服务器强制完成,客户端使用者无权拒绝升级,这样保证了客户端防病毒软件的及时更新,对新的病毒有最强的抵抗能力;

通过防病毒控制中心,限制客户端无权关闭或卸载防病毒软件,只有管理员可以停止客户端防病毒软件。强制开启客户端防病毒软件,对客户机起到病毒防护作用;

可以对客户端限制防病毒软件的使用权限,例如只能扫描本机,不允许扫描网络驱动盘等。

我们还可以通过组的定义,将不同类型的客户端分配到不同的组进行策略定制,例如笔记本用户需要在出差时去 Internet 下载病毒定义,则可以通过组划分,将笔记本用户划分到移动用户组,授予从 Internet 下载病毒定义的权利。

A5.3 内网安全及管理

在各分支部署分支核心服务器及分支控制中心;

在所有客户端部署内网安全及管理客户端代理；

利用内网安全及管理系统，对公司客户机进行资产管理，例如统计公司客户机硬件信息、软件信息、漏洞信息、补丁信息等，并可制作详尽的报表供管理员参考和总结；

软件的分发，限制客户端安装软件的类型，确保客户端只使用与工作相关的软件；

操作系统的分发，通过网内建设 PXE 服务器，并利用客户端 PXE 网络启动的功能，将操作系统镜像文件分发到客户端，提高管理员维护的效率；

利用内网管理系统，结合域，可以对客户机进行系统漏洞扫描，并安装相关的系统补丁，保证客户端系统补丁的及时更新，同时也可根据管理员自定义的补丁分发列表，进行补丁分发；

利用内网管理系统，管理员可以对客户端进行远程协助，方便管理员对庞大的计算机进行故障排除和管理，提高管理员的工作效率；

通过内网安全管理系统，对客户端外设如光驱、软驱、移动存储设备进行限制，防止员工利用这些设备泄漏公司机密；

通过内网安全管理系统，对客户端的网络连接进行限制，防止员工通过电话拨号与外界通信；

通过内网安全管理系统，对外来人员接入网络中心网络进行控制，在未经允许的情况下，外来人员的接入都被视为非法，内网安全管理系统将对其进行阻断。只有在网络中心允许的情况下，外来人员才能正常接入网络中心的网络。

A5.4 文件保护及安全审计

A5.4.1 方案设计

在各分支部署文档保护系统；

利用文件加密，对电子文档进行数字加密，任何用户都只能通过用户认证，且具备解密客户端，才能对文件进行操作；

客户端只能通过打开浏览器登录文档保护系统才可下载文档；

客户端下载的文档，必须对其具有操作权限才能进行操作；

利用文档保护系统控制用户对文档的操作，例如细化权限、只读、不能拷贝、不能打印、文件的时效等；

由管理员或者文档制作者分配文件的使用权限；

由于对文档进行加密处理，即使发生文件泄漏，窃取者也无法打开受保护的文件；

将用户对文件的操作进行安全审计，以便管理员查询或发生安全事件时查询作为法律依据。

A5.4.2 产品选型

这一类产品国内研发较多，可选范围也比较大，我们推荐前沿科技文档安全管理系统（产品型号与网络中心的相同）。

A5.5 强身份认证

采用的方法与产品与网络中心相同。

A5.6 外网防毒墙部署

A5.6.1 方案设计

我们在外网 Internet 接入的边界部署了防毒墙设备，所有客户端与 Internet 之间的流量都经过防毒墙设备扫描。

该防毒墙包括防火墙和防病毒的双重功能，利用该防毒墙实现：

利用入侵检测功能防止 Internet 入侵；

利用防火墙策略控制集团外网和 Internet 之间的通信；

利用防火墙功能发布集团 Web 服务或邮件服务（如有必要）；

利用防病毒功能，对经过防毒墙设备的 SMTP、POP3、FTP、HTTP 和 IMAP 等协议的数据包进行病毒扫描，如果发现病毒，则删除病毒或丢弃数据包；

通过防毒墙进行内容过滤或 URL 过滤，限制员工上网的范围。

A5.6.2 产品选型

根据以上方案设计，我们推荐瑞星硬件防毒墙 RSW-1000，满足实际需求，其特性如下：

- 3 个 10/100M 接口；
- 防病毒网关功能，可支持 SMTP、POP3、FTP 和 HTTP 协议，进行全面病毒扫描、拦截和清除；
- 提供了专业的垃圾邮件过滤引擎；
- 数据包状态检测过滤的防火墙；
- 内置 VPN 模块，并采用国际标准 IPSec 作为 VPN 加密、认证的协议，可以与 VPN 网关、客户端软件建立加密隧道；
- 具有良好的日志记录和日志审计功能；
- 防毒墙提供远程升级功能，并且升级以后防毒墙的配置规则会自动地保存在防毒墙的新版本中，不需要管理员进行重新配置；
- 瑞星防毒墙提供了双机热备功能。

A5.7 账号整合（可选）

随着信息系统应用的增加，账号也随之不断增多，有时一个员工需要记住近 10 个账号，这对于应用系统的使用带来了极大的不便。而账号整合的概念解决了这一大难题。利用账号整合将多应用系统的用户信息集合到一起，用户只需进行一次登录即完成了多个应用系统的认证过程，访问各个应用时无需在此认证。

账号整合系统通过将各应用系统的 LDAP 数据库整合到账号管理服务器上，用户认证经由该账号管理服务器进行认证，由此完成所有应用系统的登录。

而对于管理员，在对账号进行管理的过程中，也只需对账号管理服务器进行管理，不必再为一个员工在各应用系统的账号管理而分别对数个应用系统进行操作。

A6 服务与承诺

A6.1 硬件的服务与保证体系

服务体系包括以下几个方面：

- 成立专门的客户服务部门
- 指定专职技术负责人和商务负责人
- 建立完整的客户档案
- 客户的投诉由专人负责
- 定期通过电话调查客户对服务的满意度
- 技术人员和商务人员定期回访客户
- 技术培训

计算机系统是一项人机系统的工程，人员与技术的有效结合必须通过培训和长期实践来实现。一个系统运行的好坏，不只是与软、硬件产品和应用系统的质量有关，而且和用户在计算机应用、维护及操作方面的素质有着密切关系，因此，用户培训工作是一件极其重要的工作。

我们历来重视帮助客户对新产品及其有关的前沿技术的培训，以便用户迅速掌握目前最先进的产品知识和技术，建立可靠、稳定的维护队伍并及时得到优质的售后服务，维护用户投资的长期利益，我们会不断地向用户推出相关产品的技术课程培训及系统维护方面知识的更新和扩充。

以下为具体的培训内容：

- 关于系统安全产品基本构架知识的培训
- 关于系统安全产品日常维护的培训
- 关于操作平台使用的培训
- 关于系统安全产品常见故障即如何解决的培训

培训人员、地点、时间、具体内容将根据项目的进展另行安排。培训结束后，有关使用软件的部分将以电子文档的形式转交。

服务内容包括以下几个方面：

- 无限制的电话支持：我们具有丰富的专家资源，可以为客户提供从硬件到软件的各类技术支持。获得我们服务的客户可以在 7 * 24 内获得不受限制的求助电话支持。
- 1 小时内现场服务：对于不能通过电话解决的紧急硬件问题，我们将在接到本地客户电话后的 1 小时内，派遣经过全面培训的技术人员抵达客户现场。
- 预先通知服务：根据远程监控情况通过电子邮件把重要的技术问题预先告知客户，以防患于未然。
- 定期上门检查维护：根据客户的需要，我公司可每月派技术人员到现场检查系统的运行状况，并提供维护报告，确保系统运行良好并及时发现问题。

在系统实施服务完成之后，我们将根据与网络中心的服务协议提供以下不同方式和不同级别的支持服务。

根据实际需要和双方商定,我们将按下述不同的方式为集团提供。

方　　式	描　　述
现场服务	我们派遣人员到网络中心现场提供服务。适用范围:问题诊断、处理,使用指导和问题解答
热线电话服务	我们人员通过热线电话方式为网络中心提供服务。适用范围:问题诊断、处理,使用指导和问题解答

根据用户对问题的初步描述和紧急程度,我们将按下述不同的级别提供响应(即安排出适当人员着手解决网络中心的问题,并专注于解决网络中心的问题,直到问题解决为止)。

紧急程度	描述	响 应 时 间
1	特急	我们人员全天24小时可联络,立即响应。接到报告后立即做出安排。11分钟内进行远程诊断,力争在30分钟内解决问题,对于疑难问题在30分钟内临时解决,并在1小时内赶到网络中心现场
2	紧急	我们人员全天24小时可联络,立即响应。接到报告后立即做出安排。30分钟内进行远程诊断,1小时内解决问题。对于疑难问题在1小时内临时解决。在做出安排后2小时内保证赶到用户现场
3	一般	我们人员在正常工作时间内可联络,立即响应。30分钟内进行远程诊断,1小时内解决问题。对于疑难问题,接到报告后当天保证赶到网络中心现场
4	不急	我们人员在正常工作时间内可联络,立即响应。30分钟内进行远程诊断,24小时内解决问题

A6.2　培训内容

- 技术培训:我们将为网络中心的有关系统安全产品及网络安装和维护人员提供全方位的技术方面的培训。
- 基本培训:在系统实施服务开始前,我们将为网络中心的有关人员提供有关技术、产品和项目管理等方面的培训。
- 现场培训:在系统集成服务和系统实施服务过程中,我们将为网络中心的技术人员提供针对所安装的各个产品的有关安装、设置、管理、使用和客户化等方面的现场培训。
- 移交培训:在系统实施服务过程结束时,我们将为网络中心的技术人员提供针对所安装的各种产品的有关安装、设置、管理、使用和客户化等方面的总结性培训,目的是使网络中心的技术人员能顺利接手。

网络安装维护培训

培 训 内 容	培 训 时 间	培 训 地 点
系统安全产品使用与维护	1天	网络中心
系统安全产品优化与策略制定	1天	网络中心
系统安全产品安装与调试	1天	网络中心

A6.3 方案实施团队

网络中心系统安全项目组成员

项目管理人员

姓名	拟在本工程中担任的职务	职务	电话	有无从事类似工程经验
张三	项目经理	技术总监	13909999999	丰富
李四	项目总协调	副总经理	13908888888	丰富

主要项目施工人员

姓名	拟在本工程中担任的职务	电话	有无从事类似工程经验
王五	安全产品负责人	13604444444	丰富
刘六	安全服务负责人	13665555358	丰富
赵七	工程师	13816666983	丰富
刘九	工程师	13817777750	丰富
李二	工程师	13818888839	丰富

附录B 习题答案

第1章

1. 选择题

A　A　A　D　D　D　D　C　D　B　A

2. 填空题

(1) 入侵检测设备,防火墙

(2) 动态密码或一次性密码

(3) 虹膜,声音,笔迹

(4) 黑客

(5) 主动攻击,被动攻击

(6) 拒绝服务攻击

3. 简答题(略)

第2章

1. 填空题

(1) 所有资源,使用过程

(2) 上网内容,上网行为

(3) TCP/IP,IPX

(4) 监听模式,网关模式

2. 简答题(略)

第3章

1. 选择题

A　D　D　B

2. 填空题

(1) tcsec 标准

(2) 文件夹,共享资源

(3) 网络攻击行为,网络泄密行为

(4) Windows 服务器,工作站

(5) Guest(来宾)

(6) Administrator(管理员)

(7) 系统审计保护级,安全标记保护级,结构化保护级

3. 简答题(略)

第 4 章

1. 选择题

B　B　C　C　A　D　D　C　D　B　C　C　C　B　C

2. 填空题

(1) 保障信息安全的重要手段,防止信息泄露和失密的有效措施,提高关键信息保密水平

(2) 识别,鉴别

(3) 数字签字,哈希函数

(4) 基础设施,密钥证书

(5) 密钥管理子系统,证书受理子系统

(6) 密码编码学,密码分析学

(7) 隐写术

(8) DES

(9) 私用密钥加密技术(对称加密),公开密钥加密技术(非对称加密)

(10) RSA

(11) 哈希算法

(12) 证书颁发机构(CA)

3. 简答题(略)

第 5 章

1. 选择题

D　B　D　B　B

2. 填空题

(1) 账号,肉鸡

(2) 远程控制,隐蔽性,非授权性

(3) 系统漏洞

(4) 电子邮件,恶意网页

(5) Internet 防火墙

3. 简答题(略)

第 6 章

1. 选择题

A　D　B　C　C

2. 填空题

(1) 包过滤,应用层数据

(2) 单向导通

(3) 隔离区,非军事化区

(4) 内部网络,外部网络

(5) 路由器,用户化,建立在通用操作系统上,具有安全操作系统

(6) 静态转换,动态转换,端口地址转换

(7) 应用代理网关
3. 简答题(略)
第 7 章
1. 填空题
(1) 入侵检测系统(IDS)
(2) 异常检测,误用检测
(3) 基于主机,基于网络
(4) 事件产生器,事件分析器,响应单元
(5) 保密性,可用性
2. 简答题(略)
第 8 章
1. 选择题
D　B　C　A　B
2. 填空题
(1) 隧道技术
(2) 数据链路层,帧
(3) 网络层,包
(4) 第 3 层隧道
(5) 手工配置,密钥交换协议
(6) 伪造,被篡改
(7) AH,ESP,密钥管理协议(ISAKMP)
(8) 公钥加密
(9) MD5 和 SHA
(10) 内部网
(11) TCP/IP,应用层
(12) https
3. 简答题(略)

读者意见反馈

亲爱的读者：

感谢您一直以来对清华版计算机教材的支持和爱护。为了今后为您提供更优秀的教材，请您抽出宝贵的时间来填写下面的意见反馈表，以便我们更好地对本教材做进一步改进。同时如果您在使用本教材的过程中遇到了什么问题，或者有什么好的建议，也请您来信告诉我们。

地址：北京市海淀区双清路学研大厦 A 座 602 室　计算机与信息分社营销室　收
邮编：100084　　电子邮件：jsjjc@tup. tsinghua. edu. cn
电话：010-62770175-4608/4409　　邮购电话：010-62786544

教材名称：网络安全与管理
ISBN 978-7-302-20561-6

个人资料

姓名：__________ 年龄：______所在院校/专业：__________
文化程度：________ 通信地址：________________
联系电话：________ 电子信箱：________________

您使用本书是作为：□指定教材 □选用教材 □辅导教材 □自学教材

您对本书封面设计的满意度：
□很满意 □满意 □一般 □不满意　改进建议________________

您对本书印刷质量的满意度：
□很满意 □满意 □一般 □不满意　改进建议________________

您对本书的总体满意度：
从语言质量角度看　□很满意 □满意 □一般 □不满意
从科技含量角度看　□很满意 □满意 □一般 □不满意

本书最令您满意的是：
□指导明确 □内容充实 □讲解详尽 □实例丰富

您认为本书在哪些地方应进行修改？（可附页）

____

____

您希望本书在哪些方面进行改进？（可附页）

____

____

电子教案支持

敬爱的教师：

为了配合本课程的教学需要，本教材配有配套的电子教案（素材），有需求的教师可以与我们联系，我们将向使用本教材进行教学的教师免费赠送电子教案（素材），希望有助于教学活动的开展。相关信息请拨打电话 010-62776969 或发送电子邮件至 jsjjc@tup. tsinghua. edu. cn 咨询，也可以到清华大学出版社主页（http://www. tup. com. cn 或 http://www. tup. tsinghua. edu. cn）上查询。